Jouni Kivistö-Rahnasto

Machine safety design

An approach fulfilling European safety requirements

TECHNICAL RESEARCH CENTRE OF FINLAND ESPOO 2000

VTT PUBLICATIONS 411

Machine safety design
An approach fulfilling European safety requirements

Jouni Kivistö-Rahnasto

VTT Automation

Thesis for the degree of Doctor of Technology to be presented with due permission for public examination and criticism in Auditorium Festia pieni sali at Tampere University of Technology on April 19th, 2000, at 12 o'clock noon.

TECHNICAL RESEARCH CENTRE OF FINLAND
ESPOO 2000

ISBN 951–38–5561–9 (soft back ed.)
ISSN 1235–0621 (soft back ed.)

ISBN 951–38–5562–7 (URL: http://www.inf.vtt.fi/pdf/)
ISSN 1455–0849 (URL: http://www.inf.vtt.fi/pdf/)

JULKAISIJA – UTGIVARE – PUBLISHER

Valtion teknillinen tutkimuskeskus (VTT), Vuorimiehentie 5, PL 2000, 02044 VTT
puh. vaihde (09) 4561, faksi (09) 456 4374

Statens tekniska forskningscentral (VTT), Bergsmansvägen 5, PB 2000, 02044 VTT
tel. växel (09) 4561, fax (09) 456 4374

Technical Research Centre of Finland (VTT), Vuorimiehentie 5, P.O.Box 2000, FIN–02044 VTT, Finland
phone internat. + 358 9 4561, fax + 358 9 456 4374

VTT Automaatio, Riskienhallinta, Tekniikankatu 1, PL 1306, 33101 TAMPERE
puh. vaihde (03) 316 3111, faksi (03) 316 3499

VTT Automation, Riskhantering, Tekniikankatu 1, PB 1306, 33101 TAMMERFORS
tel. växel (03) 316 3111, fax (03) 316 3499

VTT Automation, Risk Management, Tekniikankatu 1, P.O.Box 1306, FIN-33101 TAMPERE, Finland
Phone internat. +358 3 316 3111, fax +358 3 316 3499

Technical editing Maini Manninen

Otamedia Oy, Espoo 2000

Kivistö-Rahnasto, Jouni. Machine safety design. An approach fulfilling European safety requirements. Espoo 2000, Technical Research Centre of Finland, VTT Publications. 99 p. + app. 9 p.

Keywords machine safety, safety design, risk assessment, safety requirements, hazards, risks, machine design

Abstract

Deficiencies in ergonomics and safety cause negative consequences for companies, national economy and individuals and therefore safer and more healthy products and work environments are required. Improvements in ergonomics and the safety of existing workplaces increase job satisfaction, decrease absenteeism and accidents in companies and may also have positive effects on the quality of the products of companies.

Hazard analysis and risk assessment are widely accepted in product and process design. In the European Union legislators have shifted away from the application of detailed safety requirements towards requirements for application of risk analysis by companies themselves. Manufacturers or their representatives must carry out risk assessment and take results into account in machine design (Directive 98/37/EC). The new regulations are harmonised machine safety requirements within the EU member states and make it possible to market machines throughout the EU.

Today, when the revision of the directive is being considered, it is essential to integrate current safety design procedures into systematic machine design processes in order to ensure both an acceptable level of safety in machines and feasible design efforts. This work was carried out in order to integrate European safety requirements into the systematic machine design process. At the beginning of the work, the theoretical framework was described and the first version of the approach was developed. The preliminary approach was tested and further developed in case studies. The case studies cover the redesign of two existing single machines, the design of a large materials handling system and the safety design of a new single machine.

The main benefit of the approach fulfilling the European safety requirements was the clarification of the safety design requirements and simultaneous safety design together with other design tasks. The results also indicated that the harmonised C-level standards do not necessarily cover all the essential safety problems related to the machine to be designed and therefore risk assessment is recommended even if the C-level standard is available. In addition, the risk estimation according to EN 954-1 (1997) was unreliable. Individual judgements regarding the severity of consequences and the possibility of a user to avoid accident varied drastically. Finally, the machinery safety directive (Directive 98/37/EC) mixes hazards, technical requirements and safety goals in a confusing manner. Therefore, the proposal for a new draft of the directive on machinery (Proposal for... 1998) should be changed in a such way that it clearly separates the hazards, the technical requirements and the safety goals.

Preface

This thesis was researched at Tampere University of Technology and the Technical Research Centre of Finland. The thesis suggests an approach fulfilling European machine safety requirements during systematic machine design.

I wish to express my thanks to my thesis advisor, Professor Markku Mattila, and the advisory group, Professor Veikko Rouhiainen and Dr. Markku Reunanen.

I am grateful for the efforts of Professor Arto Verho, Dr. Risto Kuivanen and Professor John Stoop, who have read the manuscript, and I thank them warmly for their valuable comments and constructive criticism concerning my work.

I am also endebted to my colleagues and the engineers in the case companies for their pleasant cooperation and valuable discussions.

For the financial support received for this study I would like to express my gratitude to the Finnish Work Environment Fund, Tampere University of Technology and the Technical Research Centre of Finland.

Finally, my warmest thanks are due to my wife Heli and to my daughter Katariina.

Tampere, January 2000

Jouni Kivistö-Rahnasto

Contents

Definitions

Accident. Unplanned event giving rise to death, ill-health, injury, damage or other loss (BS 8800 1996).

Hazard. A source of possible injury or damage to health (EN 292-1 1992).

Hazardous situation. Any situation in which a person is exposed to hazard or to hazards (EN 292-1 1992).

Incident. Unplanned event which has the potential to lead to accident (BS 8800 1996).

Machine. An assembly of linked parts or components, at least one of which moves, with the appropriate actuators, control and power circuits, etc., joined together for a specific application, in particular for the processing, treatment, moving or packaging of material (Directive 98/37/EC).

Risk. A combination of the probability and the degree of possible injury or damage to health in a hazardous situation (EN 292-1 1992).

Safety of a machine. The ability of a machine to perform its function, to be transported, installed, adjusted, maintained, dismantled and disposed of under conditions of intended use specified in the instruction handbook without causing injury or damage to health (EN 292-1 1992).

1. Introduction

Deficiencies in ergonomics and the safety of workplaces cause costs and other negative consequences for companies, national economy and individuals (Aaltonen et al. 1996). Workers in companies require safer and more healthy work environments and the customers of the companies require safer and environmentally sustainable products and services (Rahimi 1995). In many cases efforts to prevent occupational accidents are made at existing workplaces (Harms-Ringdahl 1987). However, the technical possibilities to improve the safety of the existing systems are rather limited and the cost of the changes may become high (Suokas 1993). Therefore, methods to integrate safety into product design have been developed (Østerås 1998, p. 25, Kuivanen 1995, p. 63, Reunanen 1993, p. 43, Stoop 1990, p. 23).

Customers primarily expect value, not innovations (Heinonen 1994, p. 69), and ergonomics is one property which increases product value (Cross 1989, p. 128). Improvements in ergonomics and the safety of existing workplaces increase job satisfaction, decrease absenteeism and accidents in companies and may also have positive effects on the quality of the products of companies (Kuusela 1998, p. 90, Drury 1997). Ergonomic problems and deficiencies in the quality of products often have the same causes (Eklund 1997). Hence, good ergonomics and the safety of a machine are strong selling arguments for a machine manufacturing company.

Safety and ergonomics are also a matter of ethics. An engineer has the general obligation, but also the right to protect clients and the public from dangers caused by the work of engineers (Martin & Schinzinger 1996, p. 239). This right arises from moral and ethic obligations associated with the role of engineers. Hubka & Eder (1988, p. 155) state that a designer should permanently aspire to provide the best possible ergonomic properties, including protection against hazards. When the consequences of an action can be foreseen, the designer should apply the ethics of responsibility. When the precise consequences are impossible to foresee, the designer should apply the ethics of consciousness. Therefore, the best possible knowledge and consciousness are prerequisites of responsible and ethically founded actions in ergonomics (Luczak 1998).

Basic design rules, principles and guidelines, such as clarity, simplicity and safety, are important aspects of quality engineering (Beitz 1997). However, ergonomical considerations are not necessarily integrated into design processes (Broberg 1997) and the knowledge of designers concerning safety and ergonomics is not necessarily always sufficient (Main & Ward 1992). Insufficient and unfocused training is one of the major reasons for unsuccessful quality initiatives (Brown 1995). In addition, feedback to designers is often unreliable, delayed, negative and sometimes missing altogether and designers fail to learn from the feedback (Busby 1997, Smyth 1997). An experienced designer may also assume that he knows all the requirements from experience and therefore reduces his efforts to analyse the design goals (Badke-Schaub & Frankenberger 1999, Holts 1989). On the other hand, ergonomics considerations in the early stages of design has helped design teams to focus on the perspective of the user (Montreuil 1996, Haslegrave & Holmes 1994). Therefore, safety and health considerations should be integrated into the design process on the basis of concurrent engineering (Gauthier & Charron 1995).

The planning of a design process at the beginning is characterised by uncertainty (Höhne 1997) and design decisions are made under uncertainty of possible unintended consequences (Behesti 1993). The uncertainty involves risks and project risk management together with the management of safety and health risks of products are an inherent part of a company's business risk management (Sadgrove 1996, p. 4, Ulrich & Eppinger 1995, p. 271, Wideman 1992).

The control of the risks associated with production and products should not be heavily dependent on the people at risk (Culvenor & Dennis 1997). However, inadequate attention to safety and related requirements has been one of the major reasons for project failures (Constable 1992). Deficiencies in design have caused unacceptable failures and disasters of which many could have been avoided by using systematic approaches for managing engineering design (Hales 1995). Simultaneously the requirements concerning project timescales and costs are increasing and the achievement of reduction in the timescales and costs of product design is coming to depend on improvements in the quality of the design process (Cooke et al. 1997).

Hazard analysis and risk assessment are widely accepted in product and process design (Van Aken 1997). Safety analysis has mainly been based voluntarily on benefits for the company (Rouhiainen 1993) and many manufacturing system design processes have shown very few signs of systematic safety analysis (Mattila et al. 1995). However, the application of safety analysis will continue to increase (Rouhiainen 1993). In the European Union legislators have moved away from detailed safety requirements towards requirements for application of risk analysis by companies themselves (Hale et al. 1990). Today manufacturers or their representatives must carry out a risk assessment and take the results into account in machine design (Directive 98/37/EC).

The machinery safety directive (Directive 89/392/EEC) and its amendments came to force in 1995. The directive and the amendments were joined in 1998 by a new directive (Directive 98/37/EC). In the European Union the essential health and safety requirements of the machinery safety directive (Directive 98/37/EC) has become an important project management task in machine design and manufacturing. The new regulations are harmonised machine safety requirements within the EU member states and make it possible to market machines throughout the EU. In practice the manufacturer designs and manufactures machinery according to the essential health and safety requirements of the directive, prepares the technical documentation and has a type examination carried out, if necessary. On the basis of the design and documentation, the manufacturer signs the declaration of conformity and fastens the CE mark on the machinery.

According to the New Approach, the directive sets out the central requirements (Ekelenburg et al. 1995, The New Approach… 1994). Detailed instructions are given in harmonised European standards which are broken down to three levels. A-level standards are general standards useful in designing all kinds of machinery. B-level standards deal with special safety problems, such as noise, safety distances and guards. C-level standards are related to specific machinery or groups of machinery. The standards are not mandatory and the manufacturer can apply different solutions which ensure the same or a higher safety level than the solutions presented in the standards. However, designing a machine in accordance with the harmonised safety standards ensures automatically conformity with the requirements laid down in the directive.

The essential health and safety requirements of the machinery safety directive (Directive 98/37/EC) forced many companies to compare the existing designs with the new requirements. In many cases, the existing design of a machine and related documentation were modified (Kivistö-Rahnasto 1997, Kivistö-Rahnasto & Mattila 1995). Today, when the revision of the directive is being considered, it is essential to integrate current safety design procedures into systematic machine design processes in order to ensure both an acceptable level of safety in machines and feasible design efforts.

2. Scope and objectives of the study

The scope of the study is machine safety design and the integration of the essential health and safety requirements of the machinery safety directive (Directive 98/37/EC) into systematic machine design. The objectives of this study are

- to develop an approach to machine safety design that can be used to fulfil the essential safety and health requirements of the machinery safety directive
- to integrate the approach into the systematic machine design process.

On the basis of the objectives, the empirical studies concentrate on the following questions:

Question 1: Does the application of the machinery safety directive (Directive 98/37/EC) improve the safety of machines?

Question 2: Does the current structure of the machinery safety directive support systematic safety design?

Question 3: If the answer to the Question 2 is negative, how should the structure of the essential health and safety requirements of the machinery safety directive be changed in order to support systematic machine design?

At the beginning of the work the theoretical framework is described and the first version of the approach is developed on the basis of the theoretical framework. The preliminary approach is tested and further developed in case studies. The case studies cover the redesign of two existing single machines, the design of a materials handling system and the safety design of a new single machine (Figure 1).

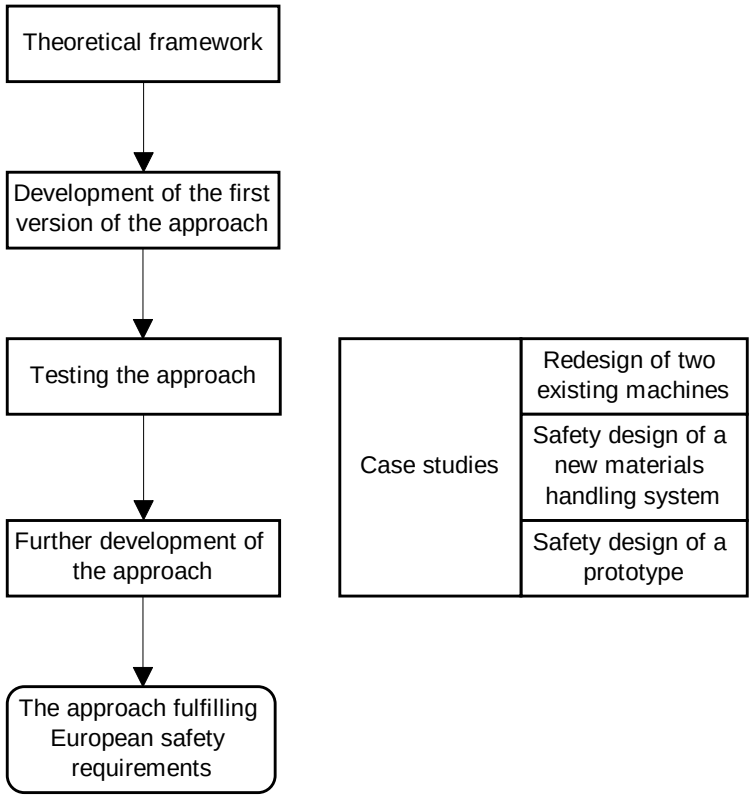

Figure 1. Phases of the development of the approach fulfilling European safety requirements in machine design.

The case studies are selected to facilitate the development of the approach fulfilling the essential health and safety requirements of the machinery safety directive (Directive 98/37/EC). The case studies also demonstrate the safety design of different kinds of machines in different kinds of design situations. However, all case studies are carried out in a business-to-business environment and no consumer products are involved. The case studies do not cover the whole spectrum of machines and design situations and this must be carefully borne in mind when generalizing the results.

3. Theoretical framework

3.1 Hazards and risks

Machine hazards are sources of potential harm or a situation of potential harm (IEC 300-3-9 1995). The hazards can cause human injuries or ill-health as well as damage to property or the environment (BS 8800 1996). The concept of hazard can also be divided into hazards and hazardous situations (EN 292-1 1992). Hazards are sources of possible injuries or damage to health and hazardous situations are any situations in which a person is exposed to hazards.

Hazards create potential conditions waiting to become loss (Roland & Moriarty 1983, p. 6). Unplanned events that cause losses are called accidents (BS 8800 1996). An accident is a dynamic mechanism that begins with the activation of a hazard, flows through the system as a series of events in logical sequences and finally produces a loss (Roland & Moriarty 1983, p. 8). If the unplanned event has a potential to lead to accident, it is incident (BS 8800 1996).

Hazards are unable to cause losses to human health, property and the environment if the chains of unplanned events are cut before the losses occur. Appropriate defences prevent the losses whereas insufficient defences enable accidents to pass through the defences and cause losses (Reason 1997, p. 11) (Figure 2).

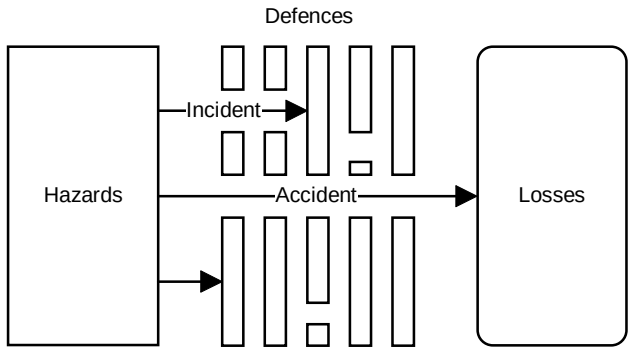

Figure 2. Hazards cause losses if the defences are unable to prevent accident (Reason 1997).

The concept of risk is essential in estimating and evaluating the significance of the losses. The risk describes the potential for realisation of unwanted and negative consequences of events (Rowe 1977, p. 24). The risk is a combination of the likelihood and the consequences of the harmful effects of a specified hazardous event (BS 8800 1996, IEC 300-3-9 1995, Vleck & Stallen 1981, Lowrance 1980). In machine design the risk is described as a combination of the probability and the degree of the possible injury or damage to health in a hazardous situation (EN 292-1 1992).

Machines must be designed according to the essential safety and health requirements on the basis of the state of the art (Directive 98/37/EC) and a manufacturer must continuously follow the technological possibilities that can be applied to improve machine safety. In addition, risks change over time (Patwardhan et al. 1990, Lowrance 1976, p. 3) and knowledge about customers' experiences of a product through its entire life cycle is essential for product quality (Johnson 1990).

3.2 Safety

Safety is a machine's ability to perform its function without causing injury or damage to health (EN 292-1 1992). A machine is safe if the risks of the machine are judged to be acceptable (Lowrance 1976, p. 75). All products involve risks and absolute safety is impossible to achieve (Jardine & Hrudey 1997, Ballard 1993, Abbot 1987, p. 43, Thomson 1987, p. 1).

The scale of risk is divided between safety and danger (Schön 1993). Things having low risk are safe and things having high risk are dangerous. Rowe (1980) suggests that when the risk increases from zero level, it may still be acceptable. When the risk continues to increase, the risk level exceeds the non-action level and risk reduction becomes desirable. At a certain point risk is unacceptable and risk reduction measures are required.

The machinery safety directive (Directive 98/37/EC) sets out the essential health and safety requirements. The machinery safety directive obliges machine manufacturers to assess the hazards of the machine to be designed and to design the necessary safety measures on the basis of this assessment. The directive and

the related standards handle machine safety and machine risks qualitatively; they provide no quantitative approach and no acceptability standard. The principle harmonised European standards for risk assessment EN 1050 (1997) and EN 954-1 (1997) provide aid in prioritizing hazards and accident scenarios, but they do not provide instructions for evaluating the acceptability of risks.

3.3 Safety in design

3.3.1 Approaches to design

Design is a purposeful human activity in which cognitive processes transform human needs and intentions into embodied objects (Roseman & Gero 1998). Design processes are not all alike. Much of designing is actually variant design (28%) and adaptive design (36%), while original design accounts for 36% of all design activities (Culley et al. 1999). Hence, most design work is a short design process under great pressure of time aiming to create a fairly good, but not optimal, design solution with minimum documentation (Günther & Ehrlenspiel 1999). On the other hand an optimal solution which is innovative, safe and low-cost, requires a longer design process and more systematic methods. Investigations have shown that various approaches to problem solving result in good solutions (Pahl & Badke-Schaub 1999). Each individual procedure has its own advantages and disadvantages and the successful use of different design strategies and methods depends strongly on the type of experience that the designer has (Weth 1999).

Dym & Levitt (1991, p. 39) describe three strategies for problem solving. The first strategy is called generate and test, in which all the possible states are systematically generated and tested to see if they satisfy the goal and constraints. The second strategy is decomposition or problem reduction. In this strategy the problem is divided into subproblems which are easier to solve than the initial problem. The third strategy is called match, in which a current state is compared with the goal and the difference between these states is defined.

Different kinds of approaches and methods in designing have been described. The decomposition or problem reduction strategy of problem solving is the basis for the methods of systems engineering (Pahl & Beitz 1996, VDI 2221 1993,

Ulrich & Eppinger 1995, Roozenburg & Eekels 1995). On the other hand, Quality Function Deployment (Akao 1988) and axiomatic design (Suh 1990) more closely match a strategy which aims to identify the factors and the design parameters that must be adjusted in order to attain customer satisfaction and design goals.

Systems engineering can be applied in the creation of new machine functions whereas Quality Function Deployment is frequently limited to improving existing functions. On the other hand, axiomatic design seems appropriate for optimisation and improving the robustness of design solutions. Therefore, systems engineering is selected as a basis for the development of an approach which aims to fulfil the European safety requirements. In this study VDI 2221 (1993) is used as a framework for the design process.

3.3.2 Safety in general problem solving

The design of a machine consists of multiple problems which must be solved in order to achieve the design goals (VDI 2221 1993). The problem-solving strategies are general and they can be applied to machine design problems as well as to safety. The identical phases of the problem solving in design (VDI 2221 1993) and the iterative process to achieve safety (EN 1050 1997) create a natural link integrating safety into machine design (Figure 3).

Problem analysis aims to gather necessary information concerning design problems (VDI 2221 1993). Ideas on how to develop a new machine and the causes behind development problems are formed in the analysis phase, together with the criteria that the new machine should meet (Roozenburg & Eekels 1995, p. 131). The losses to human health, environment or property cause design problems. Safety management can be seen as a set of problem-solving activities at different levels of abstraction (Hale et al. 1997). Safety problems are aspects of the design problem and they set new demands that are not imposed by other design criteria (Stoop 1990, p. 86).

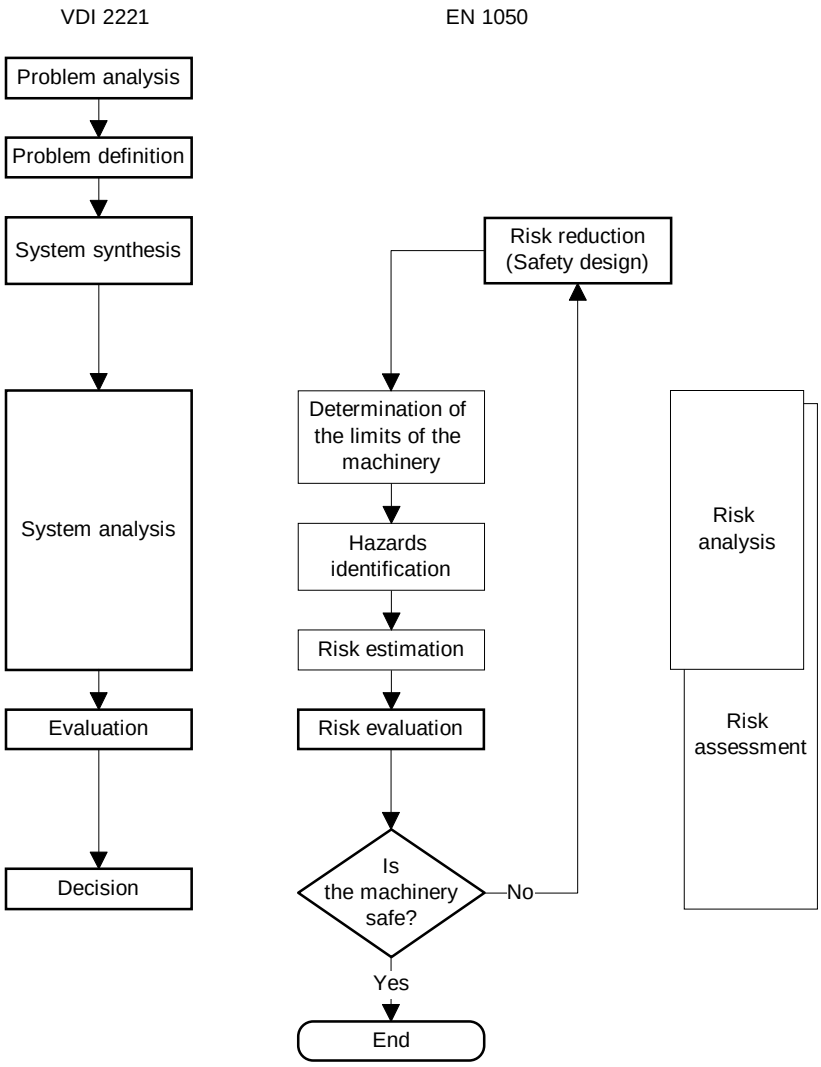

Figure 3. Comparison between general problem solving (VDI 2221 1993, p. 4) and the process to achieve safety (EN 1050 1997, p. 11).

The accident scenarios formed from use scenarios and hazards should be used as a basis of safety design (Stoop 1990, p. 56). Safety problems are typically related to existing machines and problem solving actually starts with the system analysis phase, or with risk analysis as this is called in safety design (Figure 3). In the risk analysis phase, knowledge about the machine's nature, limits and life phases, users and other people, accident and incident history and damage to

health should be gathered in order to identify the hazards of the machine and possible accident scenarios (EN 1050 1997). Especially accident analysis can provide important information about the actual accident sequences, making it possible to design appropriate safety measures to prevent hazards and losses.

The design problem must be clearly defined from a fuzzy array of facts and myths into coherent statements or questions (Suh 1990, p. 6). The problem is defined and formulated in greater detail in the problem definition phase (VDI 2221 1993). The design problem includes goals that are required to be achieved. The goals can be further elaborated into more specific objectives (Roozenburg & Eekels 1995, p. 136). Initial statements about the objectives may be vague and they need to be expanded and clarified (Cross 1989, p. 45). The list of objectives is called the design specification (Roozenburg & Eekels 1995, p. 131). In addition to hazards of the machine and the possible accident scenarios, the safety design specification should also include information concerning the people exposed to the hazards, the environment, standards and codes of practice and legal requirements (Abbot 1987, p. 77). Documentation of the constraints is one of the major objectives of the process of product specification. An underconstrained solution is not necessarily in an acceptable solution space at all (Gause & Weinberg 1989). In his example, Willem (1988) states that required attributes, like safety, describe the product properties that the design must have if it is a solution to the problem.

The requirements of the machinery safety directive (Directive 98/37/EC) concerning safety objectives, safety measures and instructions, together with the safety analysis of existing machines, creates the basis for a safety-related design specification. The essential health and safety requirements of the machinery safety directive (Directive 98/37/EC) are mandatory and therefore they must be handled primarily as requirements that must be fulfilled under all circumstances. However, all the safety objectives may not be completely satisfied by the current state of the art. Therefore laws also attempt to describe the procedures for deciding the highest possible level of safety (Hale & Swuste 1998). In those cases the machine must be designed to meet the safety objective as far as possible.

Means for satisfying the design criteria are created in the system synthesis phase (VDI 2221 1993) (Figure 3). Provisional solutions for the design problems as

well as for known safety problems are created. Solutions that cause no hazards should be applied as far as possible in fulfilling the functional requirements (EN 292-1 1992, Barnett & Brickman 1986). The risks connected with solution should be lowered to an acceptable level if total elimination is impossible. Safety devices are applied if an unacceptable risk exists despite risk reduction measures. In addition to safety devices, additional warnings, instructions and user training may be necessary.

The behaviour and properties of the provisional design solutions are studied in the system analysis phase (VDI 2221 1993). Roozenburg & Eekels (1995, p. 235) call this phase simulation. System analysis aims to determine the properties of the provisional design solutions. The safety of the suggested solutions should be analysed in order to identify and model possible dangerous behaviour and properties of the solutions. If hazards exist, valid predictions of the side effects of the design solutions should be made (Behesti 1993, Stoop 1990, p. 53, Hubka & Eder 1988, p. 48).

In the evaluation phase (VDI 2221 1993) the solutions are assessed against the initial design requirements (Roozenburg & Eekels 1995, p. 293, Nijhuis & Roozenburg 1997). The essential safety and health requirements are set in the problem analysis and problem definition phases and the provisional solutions should fulfil the requirements. The results of risk analysis can be applied to (Kjellén & Sklet 1995)

- verify the acceptability of a concept
- compare and select between concepts
- further reduce risks of a chosen concept.

It is also possible that the system analysis phase reveals new safety problems that are not covered by the initial design specification. In that case risk evaluation can be used to judge the significance of the problem. If the problem is considered significant, new design requirements have to be set.

Decisions about the acceptability of the solution or the need for better solutions are made in the decision phase. If the provisional designs are not acceptable, the decision phase leads to an iterative process (Roozenburg & Eekels 1995, p. 92, Stoop 1990, p. 68). Totally new solutions may be needed or existing solutions

are further developed. In both cases it is important to use the new safety information from the system analysis and evaluation phases in setting the new safety requirements.

3.3.3 Integration of safety into the design process

VDI 2221 (1993) divides the design process into seven stages (Figure 4). During the task clarification stage the design problem is clarified and the design specification is formed. On the basis of the design specification the inputs and outputs of the system and the functions between them are created in the determination of the functions and the function-structure stage. Function structure describes the overall relationships between different functions and subfunctions. Alternative solution principles for the functions are created in the stage “search for solutions principles and their combinations”. The optimal solution principle or several alternative concepts are selected for further development. In the next design stage the solution principles are divided into realisable modules. The design of the modules is started in the layout design of the key modules. After the layouts of the key modules have been defined, the overall layout of all the modules is completed. In the last design stage the layouts and modules are detailed and the drawings, instructions and other documents are prepared.

The design process flows from the task clarification to the detailed drawings and instructions for the manufacturing and the use of the machine. Each design stage starts with clarification and formulation of the problem and continues with the synthesis phase aiming to identify alternative solutions to the problem. The possible solutions are then analysed and evaluated against different kinds of design criteria. On the basis of the evaluation decisions about the acceptability of alternative solutions are made and the design process proceeds to the next design stage. This conforms with the iterative process for achieving safety (Figure 3). The design consists of the vertical design stages and the horizontal analysis, evaluation and decision making process concerning the proposed solutions in each design stage. Thus, the risk assessment and safety design is carried out horizontally in each design stage simultaneously with other design tasks (Figure 4).

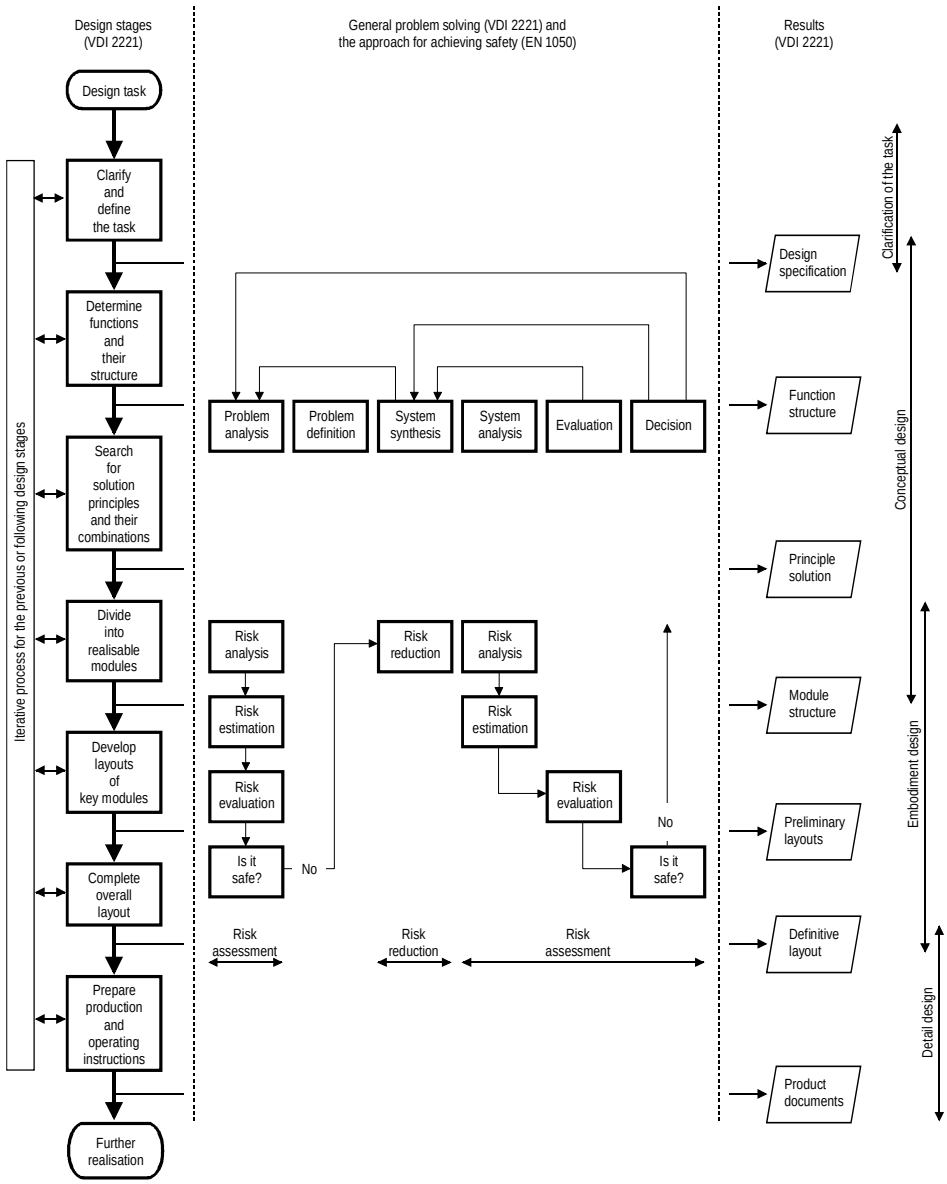

Figure 4. Integration of general design process (VDI 2221 1993) and the process to achieve safety (EN 1050 1997).

Stoop (1990, p. 24) states that the design process itself, the interdiscipline and problem orientation should be considered when integrating safety into a design process. Safety should be integrated into the design process by considering

safety problems as design problems. Interdisciplinary work is needed in order to utilise the knowledge from different disciplines and problem orientation is important to prevent overemphasising certain factors at the expense of other factors are not considered.

The safety-related decisions are made at five decision points of the design process (Stoop 1990, p. 88). The first decision point deals with the scenarios of the use of the product and requirements for the product. The requirements should be set in a general manner in order to leave sufficient solution space to enable safety improvements to be made. The second safety-related decision point is the selection of a solution principle. The solutions can be constrained by existing design and innovation, the state of technology and user acceptance, while certain technologies and energy sources involve inherent hazards that should be avoided. At the third decision point, allocation of functions between man and machine is made. This allocation should rely on expertise regarding use, user interfaces and cognition of the users. The fourth decision point is comprised of selection of the risk that will be interfered and the selection of the risk control strategy between risk elimination and risk reduction. The final decision point deals with the evaluation of the safety of the design in the long term. The residual risks and new use scenarios should be assessed on the basis of the whole lifecycle of the product. In addition, attention should be paid to changing characteristics of the user due to ageing and loss of capabilities.

Reunanen (1993, p. 43) integrated safety into a design process by applying different kinds of safety analysis in different stages of the design process (VDI 2221 1993) (Figure 4). Safety analysis was applied to yield requirements of the product or determine the safe use of the product. Product design could directly benefit from the new identified safety requirements and information concerning the safe use of the product could be used in detailed design when user instructions are composed. Similarly Østerås (1998, p. 25) applied design for X approach to assess reliability, maintainability and safety in conceptual design. The identification of the event chains causing accidents in the conceptual design phase was found to be important in identifying appropriate risk-reduction measures.

Kuivanen (1995, p. 63) applied a simultaneous and interdisciplinary design approach to the design of safety in robot systems. In the early design stages the

allocation of functions between user and automation was an essential safety-related decision. In the next design stage safety factors were considered in more detail. Built-in safety factors such as stopping procedures and ergonomics were defined and designed. Layouts, work tasks and workplaces were designed simultaneously together with the user. Applicability of safety standards and legislation was studied and obvious safety devices and functions were defined and designed on the basis of the standards. The basic solutions of the system were designed during the specifying design stage. In addition, safety and ergonomics experts compared and analysed different kinds of safety solutions on the basis of 3D animation.

4. The approach to machine safety design

4.1 The process to achieve safety

4.1.1 Phases of the process

The approach fulfilling European safety requirements consists of the design process (Figure 4) and the iterative problem-solving process to achieve safety (Figure 5). The design process is based on VDI 2221 (1993) and the safety is designed simultaneously with other properties of the machine. Each design stage (Figure 4) includes an iterative process to achieve safety (Figure 5)

- analysis of safety problem
- definition of safety problems and requirements and preparation of safety design specification
- systems synthesis and risk reduction
- analysis of risks of alternative solutions and satisfaction of requirements of the safety design specification
- evaluation of risks of alternative solutions and satisfaction of the requirements
- decision making.

The procedure is based on EN 1050 (1997) and conforms with the general problem-solving cycle described in VDI 2221 (1993). The process is repeated in each design stage until acceptable safety is achieved. The risk assessments are located in the problem analysis before the system synthesis and in the system analysis after the system synthesis. The problem analysis clarifies the safety design problem and the system analysis is carried out to evaluate the results of the system synthesis. The safety design process is controlled by the safety design specification (Appendix 3). In the system synthesis and risk reduction phase it directs the design activities and in the evaluation phase it builds up an evaluation criterion among others.

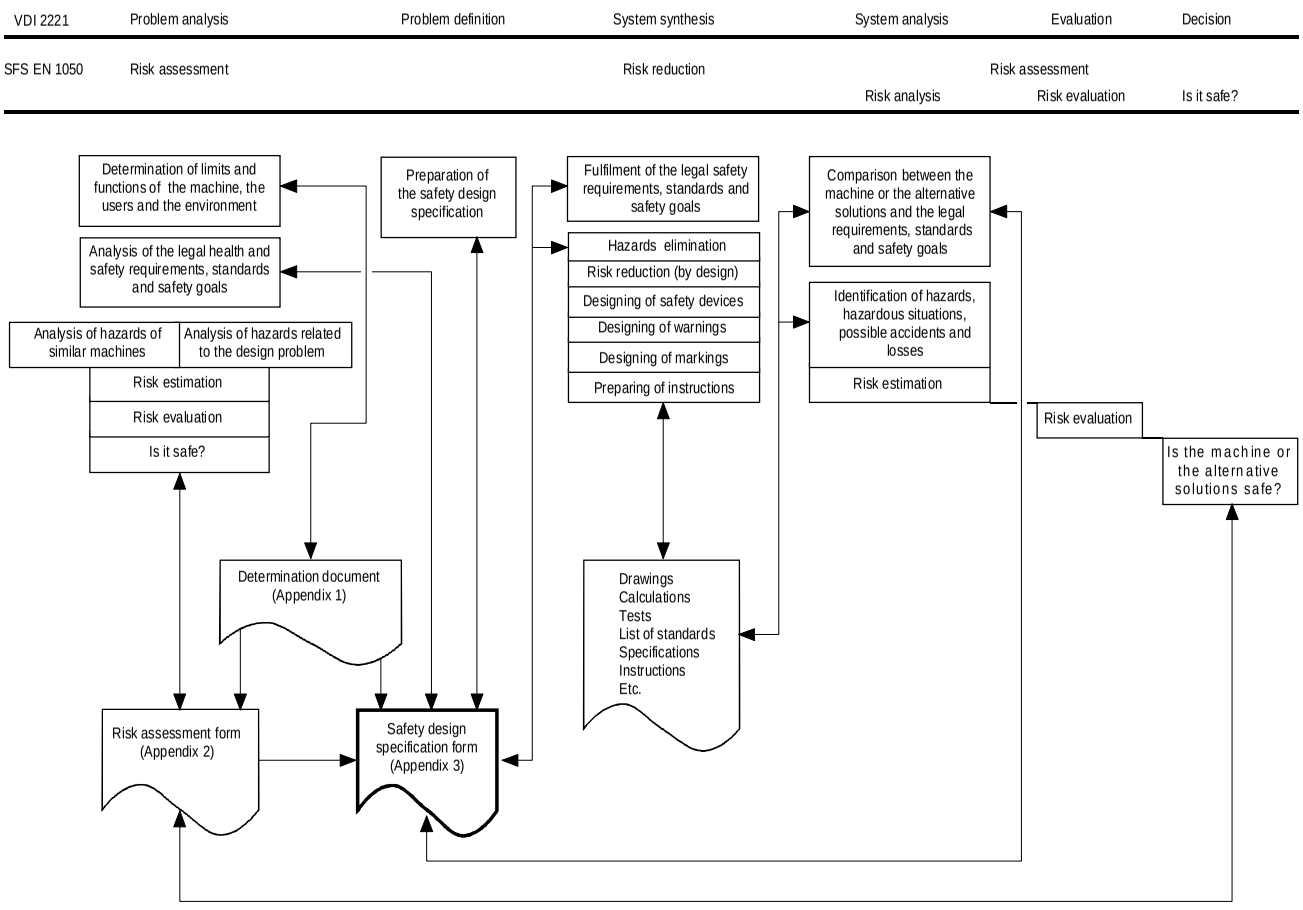

Figure 5. The process to achieve safety.

The risk assessment related to the problem analysis covers the determination of the limits and functions of the machine, the users and the environment (Figure 5). In addition, the existing legal safety requirements, standards and codes of practice are analysed and the relevant requirements are selected. The risk assessment is applied to identify the inherent risks associated with the design problem and the common risks of existing similar machines and the machine to be designed. The result of the problem analysis and the problem-definition phases is the safety design specification for the next design stage.

The system synthesis phase creates alternative solutions for the design problem. The alternative solutions for the safety problems of the machine are created and the legal safety requirements, standards and safety goals are fulfilled (Figure 5). The alternative solutions for the design problem are analysed and evaluated in a multidisciplinary fashion in order to identify the optimal solution. The risks of the solutions are one aspect involved. The assessment of the risks covers the risks of the solutions and the comparison between the solution and the legal requirements, standards and safety goals. In many cases an iterative process is needed to create acceptable solutions.

4.1.2 Risk assessment

The aim of risk assessment is to produce information about the hazards of the machine in order to create and update the safety design specification. Risk assessment requires information about the intended and unintended use of the machine, the structure and functions of the machine, the environment and users of the machine. Systematic determination of the limits and functions of the machine, its users and environment (Appendix 1) helps design teams to identify the hazards and accident scenarios to be avoided and to evaluate existing safety measures.

The machinery safety directive (Directive 98/37/EC) sets out specific requirements for safety measures. Some of the requirements consider safety measures related to specific hazards, like requirements for the fixed guards applied to prevent hazard of a moving part. These requirements enable the design team to select and design appropriate safety measures for the hazards and possible accidents that are identified. Some of the requirements are related to certain functions of the machine or to user tasks, like starting and stopping the

machine or maintenance. These requirements are relevant if the machine has the specific function or the user task. Some of the requirements, like markings, are more general and are not necessarily associated with any specific hazard or machine function or user task. Hence, all the essential health and safety requirements of the machinery safety directive (Directive 98/37/EC) cannot be fulfilled on the basis of hazard identification. Therefore, the safety analysis team must go through all the essential safety and health requirements and identify the requirements that are relevant for the machine. In addition, the requirements of the A-, B- and C-level standards should be considered. The relevant requirements are part of the safety design specification (Appendix 3).

The analysis of the legal requirements is followed by the identification of hazard and the possible accident scenarios of existing similar machines. Methods for hazard identification in early design phases are, for example, investigation of accidents and incidents that have occurred, Preliminary Hazard Analysis (PHA) and Potential Problem Analysis (PPA) (Reunanen 1993). Failure Mode and Effect Analysis (FMEA) and Fault Tree Analysis (FTA) as well as methods for checking control systems (Tiusanen et al. 1994) are typically applied to gather more detailed information about the functions, modules and components. Hazard and Operability Analysis (HAZOP) is applied in the process industry, but it can also be applied to the design of robustness of machines. Work Safety Analysis (WSA) and Human Error Analysis (HEA) as well as different kinds of usability evaluation methods and ergonomics considerations are applied to gather information about user performance.

In this approach the hazard identification is based on the general list of machine hazards (EN 1050 1997) and the results of the determination of the limits and functions of the machine. Once a hazard and the accident scenarios are identified, they are documented using the risk assessment form (Appendix 2). When necessary, the design team clarify the severity of losses caused by the hazards, frequency of the hazardous events and the possibilities of users to avoid the accident (EN 1050 1997, EN 954-1 1997). The results of risk estimation and evaluation of the acceptability of the risks are documented using the risk assessment form (Appendix 2). The safety design specification (Appendix 3) is created on the basis of the risk assessment and the comparison between the existing safety measures of the machine and the essential health and safety requirements.

After the system synthesis the risk assessment is used to evaluate the results of the design and the safety of the proposed solutions. Hence the objectives of the risk assessment differ from the risk assessments that are carried out to clarify the safety design problem. The focus is on the analysis of the new risks that are typical of the design solution and also on the evaluation of the alternative solutions. In practice the process is iterative and the risk assessment is carried out very much in the system synthesis phase.

4.1.3 System synthesis and risk reduction

The risks that are identified, evaluated and considered so important that further action is needed are removed or reduced in the system synthesis phase. The safety design is based on the safety design specification (Appendix 3) and covers the structure, functions and the use of the machine as well as warnings, markings and user instructions. The safety design specification lists the hazards and hazardous situations to be avoided and the basic requirements for the safety measures. Detailed instructions for safety measures are given in harmonised A-, B- and C-level European standards when necessary. The design team selects and designs appropriate safety measures and describes the selected safety measures in the safety design specification (Appendix 3).

The iterative safety design process for selecting appropriate preventive safety measures for the possible accidents is presented in standard EN 292-1 (1992) (Figure 6). The first safety design step is to map different kinds of possibilities for removing the source of hazard. However, all hazards are not removable. In such a case the design team should find design solutions, like reduction of electrical voltage, that reduce the risks of the possible accidents to the acceptable level. Even the risk-reduction measures may be inadequate or it may be impossible to lower the risks sufficiently, forcing the design team to design additional safety devices. If the design of safety devices is impossible, the basic concept that causes the hazard must be changed. Informing the user about the remaining risk by warnings, markings and instructions is the last safety measure. Merely informing the user, without any other kinds of actions to improve safety, is an insufficient safety measure (Figure 6).

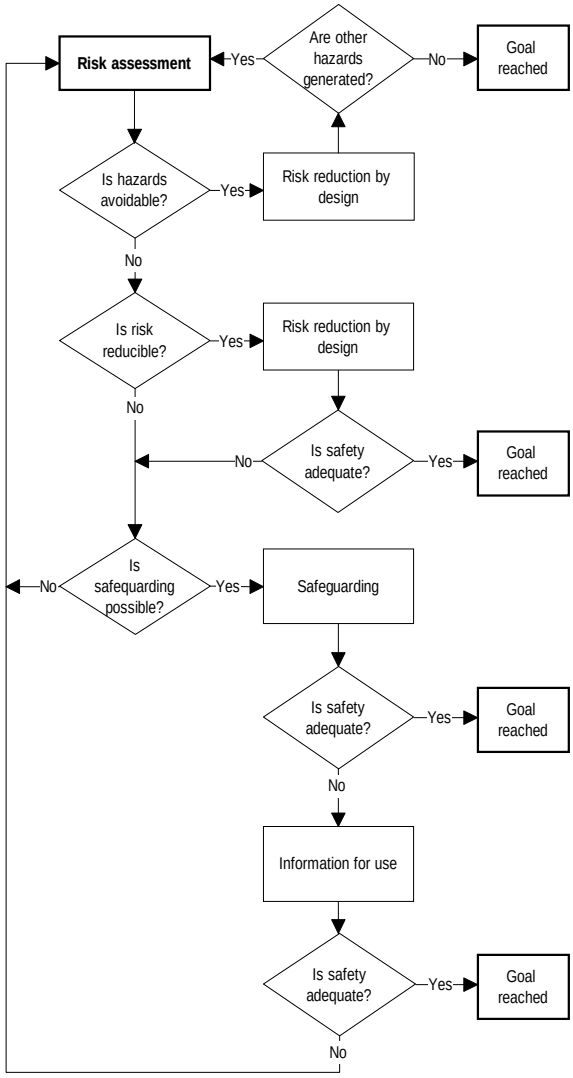

Figure 6. The iterative process of risk reduction (EN 292-1 1992).

4.2 Application of the approach in the different design stages

4.2.1 Task clarification

The task clarification stage aims to identify all available information about the hazards of the machine, about the legal and standard requirements for the safety measures and design principles and about the limits of the machine, user and environment (Table 1). In the early stages of a design project it is also necessary to evaluate the design in order to determine its feasibility and where to concentrate further work (Crossland et al. 1995). The result of the task clarification is the safety design specification.

The problem analysis and the system analysis phases are followed by risk evaluation and decision making about the acceptability of the risks of the machine (Table 1). The unacceptable risks create safety design problems and are added to the safety design specification. The functions and limits of the machine, user and environment are also evaluated and the most important limitations and requirements are added to the safety design specification. Finally, the relevancy of the legal requirements and standards are evaluated and the relevant requirements are added to the safety design specification.

The information concerning the design problem, the requirements and limitations is gathered by different methods and approaches and can overlap. For example, the legal safety requirements can cover a hazard that is identified in the analysis of existing similar machines. Therefore, the safety design specification must be gone through and simplified.

Table 1. Safety in the task clarification stage.

Process phase	**Safety design task**			
Problem analysis		Analyse the requirements of legislation and standards		Analyse the design problem Analyse the hazards related to the design problem
System analysis	Analyse the limits of the machine, users and environment		Analyse the hazards of the existing and similar machines; accidents, hazardous events, previous risk assessments, etc.	
Evaluation	Evaluate the consequences and the importance of the limits	Evaluate the relevancy of the requirements	Evaluate the risks of the hazards	
	Evaluate the acceptability of the risks of the suggested design problem Evaluate consequences and possible design problems			
Decision making	Select the appropriate limitations that must be taken into account during the design	Select the appropriate safety requirements for the machine	Select the risks that must be considered during the design	
	Decide the acceptability of the risks of the suggested design problem			
Problem definition	Define the intended use and foreseeable misuse of the machine and the environment	Define the relevant health and safety requirements of legislation and standards	Define the safety design problems caused by risks of the machine or component to be designed	

4.2.2 Determination of functions and function structure

The safety design specification is the basis for the safety design in the determination-of-functions-and-function-structure stage. The hazards, the legal requirements as well as the standards and limits of the machine, the users and the environment can be taken into account during the determination of the functions and function structure of the machine. This is important because the elimination of the remaining risks is more difficult during the following design phases (Table 2).

The machine must have the mandatory safety functions described in the machinery safety directive (Directive 98/37/EC) and in the related standards. The risks that are not covered by the mandatory safety functions must be removed or reduced as far as possible and the appropriate safety functions must be determined. In addition, the determination of functions and function structures may create new hazards and ergonomic problems that are not considered in the task clarification stages. These risks must also be analysed and taken into account during the determination of safety functions.

The remaining risks of the machine are evaluated and safety functions to protect against the risks are selected. The iterative process must be continued until the appropriate safety functions for the unacceptable risks are created and added to the safety design specification. During the risk evaluation it is also recommended to evaluate the difficulties that the design of the safety functions will cause during the following design phases.

The allocation of functions between machine and users is made during the determination phase. The allocation of functions can be applied during the following design stages in designing the ergonomics of the work tasks and the user interfaces between user and machine (Table 2).

Table 2. Safety in the determination-of-functions-and-function-structure stage.

Process phase	**Safety design task**			
System synthesis	Select the safety-related functions that are required by legislation and standards	Remove or reduce the risks that are listed in the safety design specification	Allocate functions between the machine and the user Describe the work tasks and user interfaces	Create the functions and function structures of the machine Remove or reduce risks of the functions and function structures
System analysis	Compare the functions and function structures and the safety requirements	Analyse the remaining risks of the alternative risk-reduction measures	Analyse the ergonomics of the alternative work tasks and user interfaces	Analyse the risks of the alternative functions and function structures of the machine and carry out appropriate risk removal and risk reduction
Evaluation	Evaluate the fulfilment of the requirements	Evaluate the alternative risk-reduction measures	Evaluate the ergonomics alternative work tasks and user interfaces	Evaluate the remaining risks of the alternative function structures
	Evaluate the acceptability of the risks and the possibilities to reduce the risks			
Decision making	Select the safety functions and function structures	Select the risk-reduction measures	Select the user interfaces and work tasks	Select the function structure
	Decide the acceptability of the risks			
Problem analysis and problem definition	Define the safety functions and function structures	Define the risk-reduction measures	Define the required work tasks The required user interfaces	Define the functions and function structures of the machine

4.2.3 Search for solution principles

The previous design stages describe the safety and ergonomics design problems, legal and standard requirements and the functions and function structures of the machine. In this design stage the solution principles for the safety design problems and the principles of safety measures for carrying out the safety functions are sought simultaneously with the other functions and function structures of the machine.

The solution principles for the functions and function structures may have inherent hazards that are typical of them (Table 3). The inherently safe solution principles are the most preferable. If the remaining risk after the risk reduction is unacceptable, protection measures against the risk must be taken. In addition, the user must be informed about the residual risks and necessary safety measures, about appropriate training and about personal protection equipment (Directive 98/37/EC, Ullman 1997, p. 167).

Good ergonomic design principles and the limitations of the users and the environment must be taken into account when seeking the solution principles for the work tasks and user interfaces. The basic requirements for the design of work tasks are given in legislation and standards (Shaub & Landau 1998, Dickinson 1995, Stewart 1995) and different books provide additional information about the design of work (Kroemer & Grandjean 1997, Sanders & McCormick 1993).

Table 3. Safety in the search-for-solution-principles stage.

Process phase	**Safety design task**		
System synthesis	Create solution principles for the safety measures to carry out the safety functions and the safety measures – risk reduction – safety devices – personal protective equipment – warnings – markings – instructions – training – tests.	Create solution principles for user interfaces and work tasks	Create alternative solution principles for the machine's functions and function structures Remove or reduce risks caused by the solution principles for the machine
System analysis	Analyse the risks of the alternative solution principles for safety measures	Analyse the usability of the alternative user interfaces Analyse the ergonomics of the work tasks	Analyse the risks of the alternative solution principles for the machine
	Analyse the risks of the alternative sets of solution principles		
Evaluation	Evaluate the risks of the alternative solution principles for safety measures	Evaluate the usability of the alternative user interfaces Evaluate the ergonomics of the work tasks	Evaluate the remaining risks of the alternative solution principles for the machine
	Evaluate the acceptability of the risks of the alternative sets of solution principles		
Decision making	Decide the solution principles for the safety measures	Decide the solution principles for the user interfaces Decide the work tasks	Decide the solution principles for the machine
Result	The solution principles for the safety measures	The solution principles for the user interfaces The principle work tasks	The solution principles for the machine

4.2.4 Division into realisable modules

Practical design can be carried out by dividing the solution principles into realisable modules (Table 4). In addition, modular product systematics (Pahl & Beitz 1996, p. 434) can be applied to divide machine modules into function modules and production modules. Function modules are applied to implement technical functions and production modules are designed on the basis of production considerations.

The systematic hazard-based approach to safety supports the design of function modules. A safety measure against a hazards, like an emergency stop, is a basic module and it is applied in all machines. A safety measure can also be a special module, like additional lighting, and it is applied only in the case of a special environment. Adaptive modules are applied to adapt a system to other systems. For example, the adaptive module can integrate the emergency stop of a machine with the control system of a production line. Customer-specific functions, like safety fences and walkways, are carried out by non-modules and they are designed case by case.

Table 4. Safety in the division-to-realisable-modules stage.

Process phase	**Safety design task**			
System synthesis	Divide the safety measures into realisable modules	Divide the user interfaces into realisable modules	Divide the work tasks into realisable modules	Divide the structure of the machine into realisable modules Remove or reduce risks caused by the modules
System analysis and evaluation	Analyse and evaluate the risks related to the different kinds of modules Analyse and evaluate the risks of the interrelationships between the modules Analyse and evaluate the risks of the different kinds of configurations of the modules			
Decision making	Select the modules of the safety measures	Select the modules of the user interfaces	Select the sets of the work tasks	Select the modules of the machine
	Decide the acceptability of the risks of the modules			
Result	The modules of the safety measures	The modules of user interfaces	The work tasks	The modules of the machine

The ergonomic design of work can be divided on the basis of the different work tasks that are needed to operate a machine (Table 4). Different kinds of materials handling tasks, control task, and maintenance as well as disturbance-control tasks constitute specific design problems that must be solved to ensure good ergonomics. In addition to the individual work tasks, the organisational factors related to the operation of a machine must be considered.

The user interfaces can also be divided into realisable modules (Table 4). The controls, displays and other elements of user interfaces must be designed according to good ergonomic principles. In addition, the design of the user instructions is an essential part of the design of the work tasks and user interfaces. It must be noted, however, that even if the work tasks and user interfaces are divided into smaller modules, the overall ergonomics and usability must be treated on the basis of the overall system.

4.2.5 Development of the layouts of key modules

The preliminary design of the safety measures to protect against the most important hazards is carried out during the development stage of the layouts of key modules (Table 5). The design teams determine the dimensions, materials, locations etc. of the modules of the machine only as far as is practical to get an idea of the alternative layouts. The information in the relevant standards and other specifications concerning the safety measures are applied as far as is practicable.

The risks related to the alternative layouts are analysed and evaluated and necessary risk-reduction measures are designed (Table 5). The risk analysis and the ergonomics analysis and evaluation together with the evaluation regarding the other design criteria help design teams to compare the alternative solutions and select the optimal layout.

Table 5. Safety in the development-of-the-layouts-of-key-modules stage.

Process phase	**Safety design task**			
System synthesis	Design of layouts and most critical dimensions etc. of the most important safety measures – risk reduction – safety devices – personal safety equipment – warnings – markings – instructions – training – tests.	Usability design of the most important user interfaces	Ergonomic design of the most important work tasks	Design of the layouts of the key modules Safety design for the risks caused by the layouts of the key modules
System analysis and evaluation	Conformance with the legal requirements and standards Analysis and evaluation of the risk reduction and remaining risk	Analysis and evaluation of the usability of the user interfaces	Analysis and evaluation of the ergonomics of the most important work tasks	Analysis and evaluation of the remaining risks caused by the layouts of the key modules
	Decision about the acceptability of the remaining risks of the layouts of the key modules			
Decision making	Decisions about the layouts of the most important safety measures	Decisions about the most important user interfaces	Decisions about the most important work tasks	Decisions about the lay outs of the key modules
Result	The layouts of the most important safety measures	The layouts of the most important parts of user interfaces	The most important work tasks	The layouts of the key modules

4.2.6 Completing overall layouts

The preliminary layout is completed by adding more detailed information about the modules and components (Table 6). The safety measures and the user interfaces are further designed and commercial components and equipment are selected. The work tasks and related instructions are also designed in more detail. The legal requirements and standards together with handbooks are applied to give more detailed information about safety and ergonomics for the design.

Table 6. Safety in the completing-overall-layouts stage.

Process phase	**Safety design task**			
System synthesis	Design of detailed layouts of the safety measures – risk reduction – safety devices – personal safety equipment – warnings – markings – instructions – training – tests.	Design of the user interfaces	Ergonomic design of the work tasks	Design of the layouts Safety design for the risks caused by the layouts
System analysis and evaluation	Conformance with the legal requirements and standards Analysis and evaluation of the risk reduction	Analysis and evaluation of the usability of the user interfaces	Conformance with the legal requirements and standards Analysis and evaluation of the ergonomics of the most important work tasks	Analysis and evaluation of the risks caused by the details of layouts
	Decision about the acceptability of remaining risks of the layouts			
Decision making	Decisions about the layouts of the safety measures	Decisions about the user interfaces	Decisions about the work tasks	Decisions about the layouts of the machine
Results	The layouts of the safety measures	The layouts of user interfaces	The work tasks	The layouts of the machine

The system analysis and evaluation phase consists of the risks assessment of the details of the alternative components and the ergonomic evaluations of the work tasks and the user interfaces (Table 6). The evaluation is followed by decision making in which the detailed layout is confirmed.

4.2.7 Detail design

The final production instructions, user instructions and the technical construction file are finished in the detail design stage (Table 7). The technical documentation is prepared according to the requirements of the machinery safety directive Annex 5 (Directive 98/37/EC), including the necessary drawings, calculations and tests as well as the information concerning the risk assessment and risk-reduction measures. For serial products the quality measures for maintaining acceptable safety during manufacturing are also described.

The design of the user information covers the work tasks, the user interfaces and necessary warnings and instructions for the safe operating of the machine. Therefore, the instructions and other user information are designed together with the other properties of the machine and the design and production of instructions for the use are started in the tasks clarification stage.

Table 7. Safety in the detailed design stage.

Process phase	**Safety design task**			
System synthesis	Detailed design of safety measures – risk reduction – safety devices – personal safety equipment – warnings – markings – instructions – training – tests. Preparation of the technical construction file	Detailed design of user interfaces	Detailed design of the work tasks	Detailed design of the machine Safety design for the risks caused by details
System analysis and evaluation	Conformance with the legal requirements and standards Analysis and evaluation of the overall risk reduction	Analysis and evaluation of the usability of the user interfaces Analysis and evaluation of the user instructions	Analysis and evaluation of the ergonomics of the most important work tasks	Analysis and evaluation of the risks caused by the details
Decision making	Decision about the acceptability of remaining risks, ergonomics and usability of the machine			
	Decisions about the detailed design of the safety measures	Decisions about the detailed design of user interfaces	Decisions about the detailed design of the work tasks	Decisions about the detailed design of the machine
Results	Detailed design of the machine and its safety measures, user interfaces and work tasks			

5. Development of an approach fulfilling the European safety requirements in machine design

5.1 Requirements for the approach

The approach fulfilling the European safety requirements in machine design was developed to help the design team to fulfil the essential health and safety requirements of the machinery safety directive (Directive 98/37/EC). The requirements for the approach were based on the processes for achieving acceptable safety and on the general models of design processes (Figure 7).

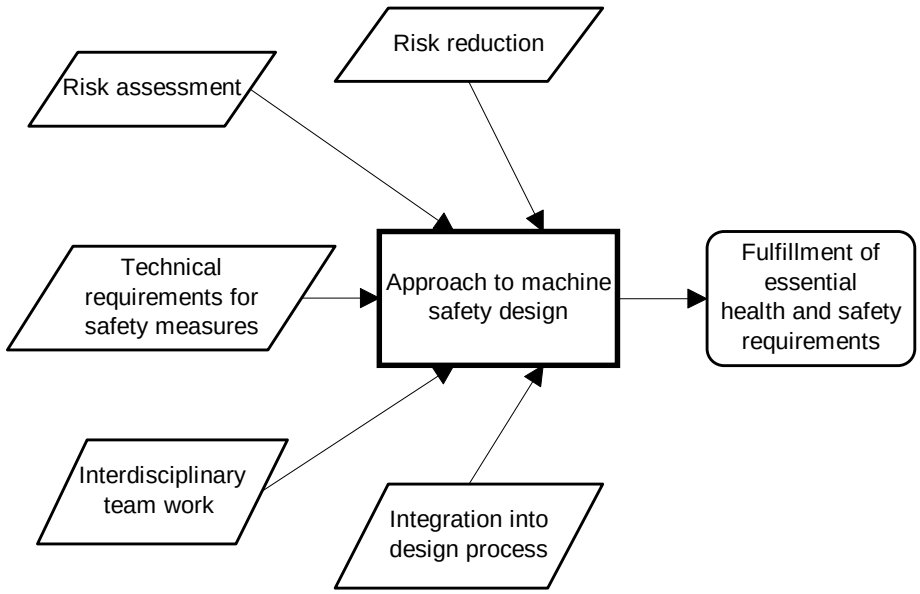

Figure 7. The framework for the development of the approach.

The machinery safety directive (Directive 98/37/EC) obliges machine manufacturers to assess the hazards of a machine and to take this assessment into account during its design. The harmonised standard EN 1050 (1997) describes a risk assessment process that can be applied to identify the hazards of a machine and to estimate and evaluate the risks of the machine in order to make decisions concerning the safety of the machine. However, the information

revealed by the risk assessment is insufficient to cover all safety requirements. Therefore, the essential health and safety requirements of the machinery safety directive Annex 1 (Directive 98/37/EC) must be taken into account during the design process.

The design of safety measures should not be separated from the overall design of a machine. Therefore, the approach is based on interdisciplinary teamwork in order to utilise the knowledge from different disciplines (Stoop 1990, p. 24) and to design the safety measures simultaneously with the other functions of the machine (Kuivanen 1995, p. 63). Safety is integrated into a general model of the design process (VDI 2221 1993) by considering safety problems as design problems (Stoop 1990, p. 86).

5.2 Phases of development

The development of the approach was carried out in four phases (Figure 8). In the first development phase, the author drafted a procedure for hazard identification according to standard EN 292-1 (1992) and EN 414 (1992). The procedure was tested in safety design of a food mixing machine. The hazard identification procedure was further developed on the basis of experience. Special attention was paid to the identification of the limits of the machine and its use and to documentation of the results. Furthermore, the requirements for safety measures were considered according to the machinery safety directive (Directive 98/37/EC).

In the second development phase the approach fulfilling the European safety requirements was applied in safety design of a colour tinting machine (Figure 8). In this stage the resources needed to carry out safety analysis and to create a safety design specification were studied. The approach was also improved according to the experience gained. The parts of the machinery safety directive concerning hazards identification were separated from the technical requirements for the safety measures. This separation made it possible to create a clear safety design specification in two stages. In the first stage hazards and hazardous situations were identified. In the second stage the design specification was completed by comparing existing safety measures with the requirements laid down in the machinery safety directive.

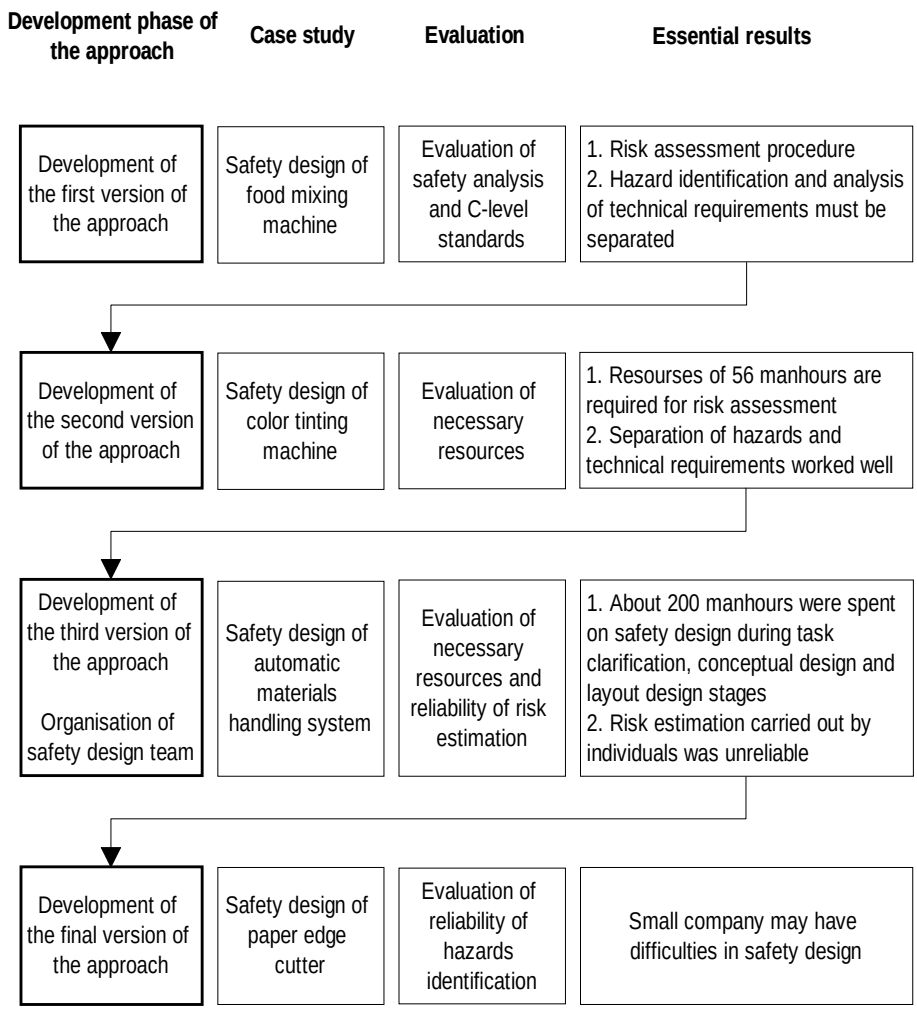

Figure 8. Development phases of the approach fulfilling the European safety requirements in machine design.

The third development phase consisted of the application of the approach to the design of a large automated materials handling system and to the evaluation of the reliability of risk estimation (Figure 8). The safety design process was organised according to principles of concurrent engineering. The risks caused by the system were estimated by the design team members and results were analysed. In addition, the technical requirements for safety requirements were considered on the basis of the machinery safety directive.

In the fourth development phase the approach was applied to safety design of the prototype of a trim cutting machine. The machine manufacturer was a small company with limited development resources. In this case study the reliability of hazard identification was evaluated and the experience concerning the applicability of the method for a small company was evaluated (Figure 8).

6. Case 1: Safety design of a food mixing machine

6.1 Introduction

Safety of a food mixing machine was designed. The original company manufacturing the machine was bought out by a new company. The new company planned to continue production according to the original design, but it had realised that the new requirements of the machinery safety directive (Directive 98/37/EC) might effect the machine causing uncertainty about safety of the machine and the company wanted to ensure safety of the machine and conformance with the directive before it started large scale manufacturing. The risk assessment was carried out in 1994, just before the machinery safety directive came into force.

The aims of the case were

- to suggest necessary changes to both the mixer and its documentation in order to create the preconditions required for signing of the EC Declaration of conformity
- to gain experience of standardised risk assessment and application of the machinery safety directive.

6.2 The food mixing machine

The food mixing machine (Figure 9) is used in food factories. The mixer consists of two rotating mixing shafts. The shafts are rotated independently by two electric motors and are located horizontally in the mixing container, the volume of which is 1.5 m^3. The container is covered by a pneumatically powered lid.

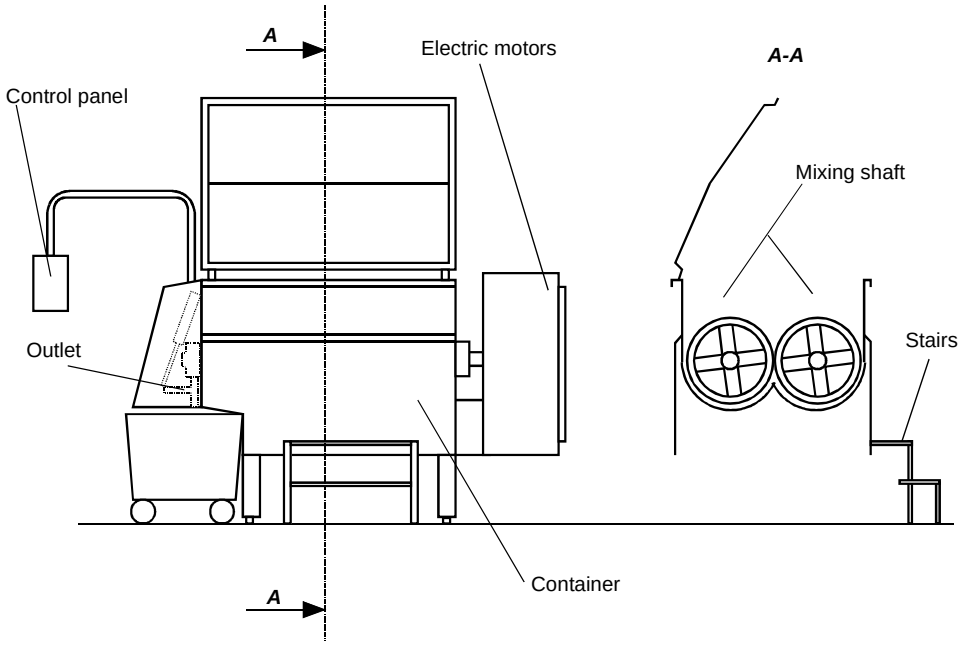

Figure 9. The food mixing machine.

The machine is operated by skilled workers. The operator uses the control panel to operate the machine. A typical work task starts by opening the pneumatically powered lid and by shutting the outlets. Food material is then poured into the container, the lid is closed and the mixer is started. The operator can control the rotation speed and the direction of the mixing shafts manually or select an automatic mode. After mixing, the mixed food material is poured into movable containers through the pneumatically powered outlets.

6.3 Method

The safety design of the food mixing machine was a typical adaptive design task. The basic concept remained unaltered and necessary modifications were carried out to fulfil the new requirements of the machinery safety directive (Directive 98/37/EC). The hazards of the old version of the food mixing machine formed the design problem. In addition, the design team had to add the essential health and safety requirements of the machinery safety directive

(Directive 98/37/EC) to the design specification. The design team consisted of a mechanical engineer, an electrical engineer and the author.

The safety design project started with basic safety training for the designers and salespersons. The safety training covered the basics of the new European machine safety legislation. In addition training was given in the requirements for the design process and the documentation together with the basic methods and procedures to assure the safety of the machine.

The risk assessment was located in the task clarification stage of the machine design process (Table 1). The mechanical designer and the author analysed the limits of the machine, the users and the environment (Appendix 1). After that, the designer and the author carried out the risk assessment of the old version of the machine. An electrical designer provided consulting for the designer and the author when necessary. The risk assessment was carried out according to standard EN 292-1 (1992). Hazard lists of the draft standards CEN/TC153/SN1 (1992) and CEN/TC153/WG2/N5.4E (1991) were also used to facilitate hazard identification.

On the basis of the risk assessment, several safety measures were suggested. In addition to safety, hygiene requirements were examined by comparing the mixer with requirements of draft standard CEN/TC153/HN124E (1993). The mechanical designer and the author also compared the machine with the essential health and safety requirements of the machinery safety directive (Directive 98/37/EC). Finally, the author compared the list of hazards of the draft standard prEN 13570 (1999) with the results of the risk assessment.

6.4 Hazards of the food mixing machine

According to the TAPS accident database of the Finnish Ministry of Social Affairs and Health, food mixing machines have cut off a user's finger in 7 accidents between 1989 and 1999. Three of the accidents (1989, 1991 and 1993) happened when a user was emptying a mixer. Two accidents in 1993 and 1995 were connected with cleaning of a machine and two accidents in 1989 and 1990 were connected with removing of meat from a mixing shaft. In addition to the

accidents, in 1992 a failure of a connector between pneumatic hose and cylinder caused the lid of a mixer to fell closed. Fortunately user was not under the lid.

Hazard identification revealed 47 hazards. The biggest hazard category was moving parts and power transmission together with machine actuators. A total of 97 hazardous situations were related to the hazards.

The mixing shafts are the most dangerous objects of the machine and cause different kinds of shearing and crushing hazards. They also involve nipping points and entanglements. The user can sway to the blades when pouring materials into the running mixer or become entangled in the mixing shafts when facilitating the mixing with a stick. The draft standard prEN 13570 (1999) did not take into account the facilitating handtools that a user can use. The mixing shafts can also cut the user's hand if the user helps the emptying of the container through the outlet by hand.

The risks of the mixing shafts are especially high during the cleaning of the machine, when the water hose or the handle of the cleaning brush can become entangled in the mixing shafts and draw the user to the shafts or strangle the user against the machine structures. In addition, unexpected start-up during the cleaning of the container causes immediate danger of death. The unexpected start-up of the mixing blades can also cause the crushing of the user's hands when the user is cleaning the shaft gasket. The draft standard prEN 13570 (1999) did not take into account these hazards related to the actual work tasks.

The uncontrolled fall of the lid of the container can cause a severe blow to the user's head, shoulder or hands. The lid and its mechanism can also cause crushing hazards between the lid and container or control panel and between the mechanism and surrounding structures. Similar hazards are caused by the outlets. The uncontrolled movements can be caused by a pneumatic failure. These failures, which are typical of pneumatic systems, are not mentioned in prEN 13570 (1999). In addition, the pneumatic hazards are ignored, although the hydraulic hazards are mentioned, in prEN 13570 (1999).

The mixer blades are powered by two electric motors and the linear movements are powered by pneumatic cylinders. The power transmission with belts, wheels and shaft gives rise to nip points and causes severing and crushing, while the

pneumatic cylinders can cause unexpected movements set up by the compressed air. Most of the hazardous situations are related to the maintenance of the machine. Typically the moving parts are started up unexpectedly due to neglect, isolation of energy sources or insufficient dissipation of the pneumatic energy. These hazardous situations were not mentioned in prEN 13570 (1999).

The work environment can be cold and wet and water, raw materials and washing detergents can make the floor and the walkways slippery. The cold environment and slippery floors increase the risk of strain during materials handling. In addition, slipping on a wet and greasy floor can cause severe injuries. The hazards caused by slippery floors, walkways and working platforms are not mentioned in prEN 13570 (1999). However, the prevention of falls and slipping on working platforms is mentioned in the safety requirements of prEN 13570 (1999).

Food material must be safe for consumers to eat and handling of the material must be safe for the workers in the food factory. In order to maintain the microbiological safety of the food, the mixer must be easy to clean, the rinsing of the machine must be easy and no contamination of the materials is allowed. The food materials can also cause health problems for the workers. The workers can be exposed to flour dust, spices and other raw materials that can cause irritation, allergy and other occupational diseases.

6.5 Risk reduction

On the basis of risk estimation, 52 hazardous situations were evaluated as being so important that safety improvements were suggested. Most improvements were related to instructions and included information about safe operation procedures, such as how to isolate the machine from its energy source and how to dissipate pressure in the pneumatic system safely. Twenty suggestions were made to improve safety by changing the structure of the mixer. Personal protective equipment was suggested for when a user handles certain raw materials

The structure of the mixer differed from draft standard CEN/TC153/HN124E (1993) in 28 points. Most of the differences (13) were located in the food

contact area. Splash areas of the mixer differed from the draft demands in nine points and six differences were found in the non-food area. A total of 21 suggestions to improve the cleanability of the mixer were made.

6.6 Discussion

Risk assessment made it possible to improve the safety of the industrial food mixing machines and it thus had a positive effect on the quality of the machines. Safety consideration also clarified the design requirements. The experience gained indicated that many safety standards are good tools facilitating practical machine design. However, all the hazards and especially hazardous situations would not have been identified if only C-level draft standards prEN 13570 (1999) were applied. The draft standard covered well the hazards caused by the moving parts of the mixing machine. On the other hand, the draft did not cover the actual hazardous situations, like failure of the pneumatic system, at all. Therefore, the designers should always carry out the risk assessment according to the A-level harmonized standards even if C-level standards are available.

The risk assessment procedure suggested in this study identified hazards and hazardous situations well. There are several limitations which must be noted when applying the risk assessment. The subject of the study was redesigning of an existing machine. Thus it was relatively easy to determine user performance and functioning of the machine. No experience was obtained on how the procedure would have worked in the design process of a new machine on the basis of drawings and models.

The essential health and safety requirements of the machinery safety directive (Directive 98/37/EC) are presented according to the hazards of machines. The obligations of the directive apply only if the corresponding hazard exists in the machine to be designed. Hence, the first step should be the identification of the hazards of the machine. In practice it is difficult to apply the directive to hazard identification because the hazards and the technical requirements are mixed. Therefore it is recommended to separate clearly the parts of the essential health and safety requirements related to hazards from the safety goals and the technical requirements for the controls, guards and protection devices, maintenance and indicators. The new proposal for a directive on machinery

(Proposal for a new… 1998) also lacks a clear division between hazards and related safety measures. In order to facilitate the hazard-based selection of safety measures, the author separated the hazards from the essential health and safety requirements (Appendix 4).

7. Case 2: Safety design of a colour tinting machine

7.1 Introduction

A manufacturer of a colour tinting machine realised that it must apply the machinery safety directive (Directive 98/37/EC) to the machine. The manufacturer decided to carry out a systematic risk assessment for the machine and to modify the machine to conform with the new health and safety requirements. Although no systematic risk assessment had been applied during the initial design process, the hazards of the machine had been considered by individual designers and several safety measures had been taken to ensure safety of the machine. In addition, the electrical system had been inspected by a Finnish electrical inspectorate.

The aims of the case were

- to create the safety design specification for the colour tinting machine in order to modify the existing machine to conform with the new health and safety requirements
- to estimate the manhours that are needed to carry out the risk assessment and to create the safety design specification
- to evaluate the benefits of the separation of the risk assessment and the comparison between the machine and the technical safety requirements.

7.2 The colour tinting machine

The colour tinting machine is used to tint paints in different colours (Figure 10). The machine is typically located in a hardware store or a paint store. The machine is operated by a store-keeper or a sales assistant having appropriate training and guidance for the operation. Typical tasks of the operators are to bring a paintbox to the machine, punch the cover of the paintbox and type the colour code on the machine's keyboard or select the colour code from a computer database. The colour tinting machine adds colorants to the paint through a hole in the cover. Finally, the operator inserts a bung in the cover hole and brings the paintbox to a blender.

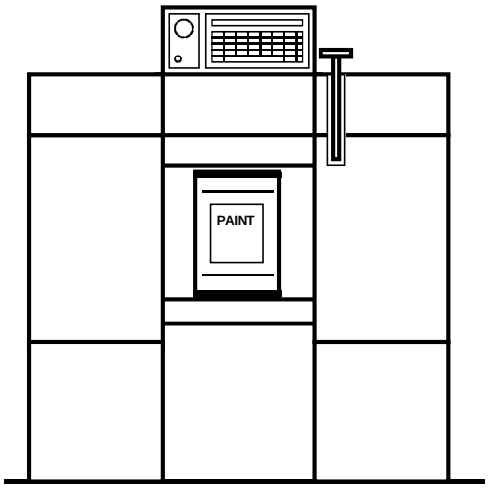

Figure 10. The colour tinting machine.

The colour tinting machine is a serial product. The machine consists of a frame, colorant containers, agitators for the colorants, a measuring pump module and a control system. Colorants are stored in the colorant containers covered with lids and equipped with agitators to prevent the colorants from forming sediment. The operator adds colorant to a container by opening the lid and pouring the colorant into the container. The colorants are measured and injected into the paintbox by the measuring pumps. The pumps are controlled by the control system. The operator can use the keyboard of the colour tinting machine to manually insert a colour code in the control system or he can select a colour from the computer database and automatically transmit it to the control system.

7.3 Method

The design task was limited to modifying the existing colour tinting machine to fulfil the essential health and safety requirements of the machinery safety directive (Directive 98/37/EC). The case was a typical adaptive design task where the basic concept remains unaltered and minor modifications are carried out to fulfil the new requirements. The hazards of the existing colour tinting machine and the technical requirements of the essential health and safety requirements of the machinery safety directive (Directive 98/37/EC) were the design problem. Other aspects, like functionality, costs and manufacturability,

were considered as evaluation criteria for the suggested safety measures. The safety design team consisted of a project manager, four designers, an experienced serviceman, and the author.

The safety design project was started with the basic safety training for the designers and salespersons (see case 3). The risk assessment was located in the task clarification stage of the machine design process (Table 1). The limits of the machine, the users and the environment were analysed, the hazards of the existing machine were identified and the machine was compared with the essential health and safety requirements of the machinery safety directive (Directive 98/37/EC).

The author, the project manager and the experienced serviceman determined the limits and functions of the machine, the user and the environment. The project manager and the serviceman both described the tasks of the machine and its operators to the author for two man hours. In addition, the author used four manhours to document the results (Table 8).

Table 8. Time used in risk assessment.

Analysis phase	Resources [manhours]	
	Author	**Company**
Determination of the limits and functions of the machine and user	8	4
Identification of the obvious hazards	8	
Risk assessment by the team	7	18
Comparison between the machine and the essential health and safety requirements	7	4
Total	30	26

The author identified the obvious hazards and hazardous situations of the colour tinting machine. The analysis of the obvious hazards lasted eight manhours (Table 8). After that the author introduced the obvious hazards to the project manager, the four designers and the service man. The team identified more hazards and hazardous situations and prioritised the hazardous situations on the basis of the severity of the consequences, the frequency of the hazardous situations and the possibility of the operators to avoid the hazards (EN 1050

1997, EN 954-1 1997). The team selected the risks to be intervened and suggested preliminary safety measures against the risks. The author used a total of seven manhours in the risk assessment with the team. The company used 18 manhours for risk assessment carried out by the team (Table 8).

The author and a mechanical designer completed the safety design specification by comparing the existing machine with the technical parts of the essential health and safety requirements of the machinery safety directive (Directive 98/37/EC). The author used seven manhours and the designer used four manhours in the comparison.

7.4 Hazards of the colour tinting machine

A total of 63 possible hazards and related hazardous situations were revealed and evaluated during the risk assessment (Table 9). The moving parts and actuators of the machine caused 38% of the hazards. A typical hazardous situation is, for example, an unexpected start-up of the machine during cleaning. The pump module can move unexpectedly and cause a bruise on the cleaner's finger if somebody starts the machine during the cleaning. To prevent unexpected start-ups, it is advised to switch of the machine and pull out the electric plug before cleaning. The same instruction is also valid for all maintenance or repair tasks.

The materials caused 33% of the machine's hazards. For example, an evaporated hazardous solvent can cause harm to the operator's health. To minimise the evaporation, colorants are added to paintboxes through a small hole. The operator punches the cover of the paintbox just before the colorants are added and inserts the bung in the cover hole after the colorants are added. In addition, the customer must ensure that local ventilation is sufficient and that the risks of the solvents are controlled and known to users.

Table 9. Number of hazards and hazardous situations of colour tinting machine.

Hazard	Number of hazards and hazardous situations	%
Moving parts, power transmission and actuators	24	38
Materials and products	21	33
Work environment and walkways	10	16
Lifting and materials handling	7	11
Energy	1	2
Total	63	100

The deficiencies in the customer's work environment can cause health problems and danger for the operator when operating the machine. These hazards cause 16% of all hazards and they are typically related to insufficient lighting or ventilation. Narrow walkways, a confined workplace and a slippery floor are also typical sources of hazards. To improve safety and comfort of the use in the colour tinting machine, the machine manufacturer can describe the advisable conditions for the working environment.

Lifting and materials handling caused 11% of the hazardous situations. For example, lifting of heavy paintboxes in twisted postures can cause fatigue and strain. Low lifting height, solid tables and shelves, good working posture and reasonable size and weight of the paintboxes reduce the risk of injury.

The failures of electrical systems cause hazardous situations in all operation tasks. Electrical shock is most probably during maintenance and repairing. To prevent electrical hazards, standard EN 60204-1 (1998) was applied and repairing of the machine is allowed for authorised personnel only.

7.5 Risk-reduction measures

The safety design was based on the safety design specification. To complete the safety design specification, two kinds of information were integrated. The hazards of the colour tinting machine were identified and evaluated in the risk

assessment. The hazards cause safety problems and they were added to the safety design specification. The safety problems must be solved during the safety design process. In addition, the existing safety measures were compared against the essential health and safety requirements of the machinery safety directive (Directive 98/37/EC). The deviations between the machine's safety measures and the essential health and safety requirements were added to the design specification to modify the existing measures in order to fulfil the new requirements.

The safety design specification included 31 suggestions for improving safety (Table 10). Modification of user instructions and warnings covered 68% of all suggestions for improving safety. The new information considered transportation, good work environment, slippery floors, paints, ergonomic handling of paintboxes, emergency stop and isolation of energy, among others.

Table 10. Number of suggestions for improving safety.

Suggested safety measure	Number of suggestions	%
Instructions	18	58
Risk reduction by design	9	29
Warnings	3	10
Inspection of electrical system	1	3
Total	31	100

The modification of the machine covered 29% of the suggestions. On the basis of risk evaluation, electrical hazards were considered the most dangerous. Therefore, careful attention was paid to design of electrical systems on the basis of EN 60204-1 (1998). In addition, voluntary inspection of the electrical system was suggested.

Moving parts of the colour tinting machine are able to cause bruises on fingers. To prevent the bruises, clearances between moving parts, safeguards and safety distances were designed. Unexpected start-ups of the machine were prevented by designing the control system according to EN 60204-1 (1998) and the emergency stop according to EN 418 (1993).

7.6 Discussion

The author, the project manager, the four designers and the serviceman created the safety design specification that was applied to modify the colour tinting machine in order to fulfil the essential health and safety requirements of the machinery safety directive. The suggested safety design tasks were relatively simple and no further risk assessments were carried out during the actual design process.

The significance of the improvements to safety is difficult to evaluate. The new hazards that were identified did not cause severe harm to human health and safety. In addition, no severe accident was reported. Therefore, the direct improvement to safety was not necessarily significant. On the other hand, the safety design requirements were clarified and documented. This information improved the design specification and thus had a positive effect on the quality of the design process. The clear safety design specification can also be applied during the next modifications and development phases of the machine, having a positive effect on the quality of the machine in the long term.

The design specification included 31 safety improvements and the creation of the safety design specification required 56 manhours of work. Average resources used to create a safety requirement in the specification was about two manhours. Reunanen (1993, p. 103) has presented that the average time to create an accident scenario is 3.3 hours, which is more than that used in this case. The reason for the different use of resources is that he analysed more complex and demanding machines having more severe consequences.

The systematic determination of the limits and functions of the machine, the users and the environment helped the author to become familiar with the machine in a short period of time. It also helped the safety design team to keep in mind different aspects of the machine, users and environment during the risk assessment. During the risk assessment it was difficult to identify all hazardous situations related to the hazard. Therefore, all possible accident scenarios were not studied if the appropriate safety measure eliminated the hazard.

In addition to hazards and hazardous situations, the safety design specification included the technical requirements of the machinery safety directive. These

requirements that are not directly associated with specific hazards are difficult to manage during the risk assessment where the focus is on hazards and hazardous situations. Instead, the approach whereby hazard identification and identification of the technical requirements are considered as separated tasks was successful when compared with the experience in the case 1.

8. Case 3: Safety design of a materials handling system

8.1 Introduction

A large automatic materials handling system for a TV screen factory was designed and manufactured. A contract was signed in 1994 but the system was delivered in 1995. The manufacturer and the customer did not pay regard to the new health and safety requirements of the machinery safety directive (Directive 98/37/EC) in 1994. However, during the project the manufacturer and the customer realised that the legislation had been changed. The new situation forced the company to become acquainted with new safety verification procedures and to apply the essential health and safety requirements of the machinery safety directive (Directive 98/37/EC).

The aims of this case were

- to fulfil the essential health and safety requirements of the materials handling system
- to test the approach in designing a large system
- to evaluate the reliability of risk estimation.

8.2 The materials handling system

The system consists of five gantry robots and seven conveyors. The task of the system is to move the moulded front panels of TV screens to a welding machine and then to a cooling oven. A conveyor moves the moulded front panels to the divider unit. The divider unit loads the front panels onto the right or left roller conveyor. The right and left sides of the system are identical and therefore only the functioning of the right side is described. The right roller conveyor moves a front panel to the loader of the welding machines. The loader picks up the front panel and loads it onto one of the welding machines. The welded front panel is moved to the buffer conveyor by the unloader. The buffer conveyor moves the front panel through the panel marking device to the lehr loader and the lehr loader moves the front panel to the cooling oven. The front panel can also be picked up from the buffer conveyor by the gauge loader, which moves the front panel to the quality control station. The measured front panel is then moved to the lehr loader by the gauge conveyor.

8.3 Method

8.3.1 Safety design

The systematic safety design was started when the layout of the key modules of the robot system was developed. The design team was starting to complete the overall layout (Table 6) and it was practically impossible to make radical changes to the layout or to change the basic solution principles. In this design stage the design team should have had a clear vision of the hazards of the system and the essential health and safety requirements of the machinery safety directive (Directive 98/37/EC) concerning the robot system in order to select and complete the appropriate safety measures.

The design team had already designed many safety measures, like safety fences and emergency stops, to protects against some obvious hazards of the robot system. However, insufficient knowledge about the safety requirements, safety design procedures, documentation and responsibilities described in the machinery safety directive (Directive 98/37/EC) confused both the design team and the customer causing unnecessary tension between the manufacturer and the customer. In order to complete the safety design and to create the necessary documentation about the safety of the system, the design team carried out a systematic risk assessment and compared the system with the essential health and safety requirements of the machinery safety directive (Directive 98/37/EC).

A concurrent engineering approach was applied to integrate safety in the design process. Five major steps were taken: 1) the project manager and designers helped the author become acquainted with the system, 2) the safety team was built up, 3) teamwork was organised, 4) practical analysis and design were put into practice and 5) sales engineers, project managers and designers learned the basics of the machinery safety directive (Directive 98/37/EC). In addition, safety engineering was taught to the designers.

The safety team consisted of a project manager, an electrical engineer, two software engineers, a pneumatic engineer, a service manager and the author. Five of the team designers and managers had strong field experience in designing, using and servicing automatic systems in different kinds of environments. One software engineer had relatively short experience of the

robotics systems in TV factories. The author had no previous experience of robot systems in TV factories.

The safety teamwork was overseen by the author, who prepared and documented all safety sessions. The safety team worked in two ways. It selected a division of the system to be analysed and the author identified the obvious hazards of the selected division. After that, the safety team collected and the author introduced the obvious safety problems. Thus, during the safety sessions, designers had the possibility to concentrate on more complex and difficult safety problems, while the obvious hazards and safety measures were already identified by the author. During the safety teamwork, the hazard identification was immediately followed by a preliminary solution the detailed design of which was given to a team member. If the preliminary solution was not found within a reasonable period of time, the solving of the problem was given to a team member who then built an appropriate team to solve the problem. The customer's view, mostly that of the production managers, was listened to concerning all major safety aspects (Figure 11).

In addition to practical design, two training programs were carried out. The first package dealt with the machinery safety directive (Directive 98/37/EC) in general. The target group was the sales engineers, the project managers and the designers. The aim of the first package was to learn basic procedures related to the machinery safety directive. This kind of training is important for supporting communication between different departments and individuals in the company. For example, it is important that the marketing and the design departments share the same concepts concerning the CE mark and the procedures and requirements behind the mark.

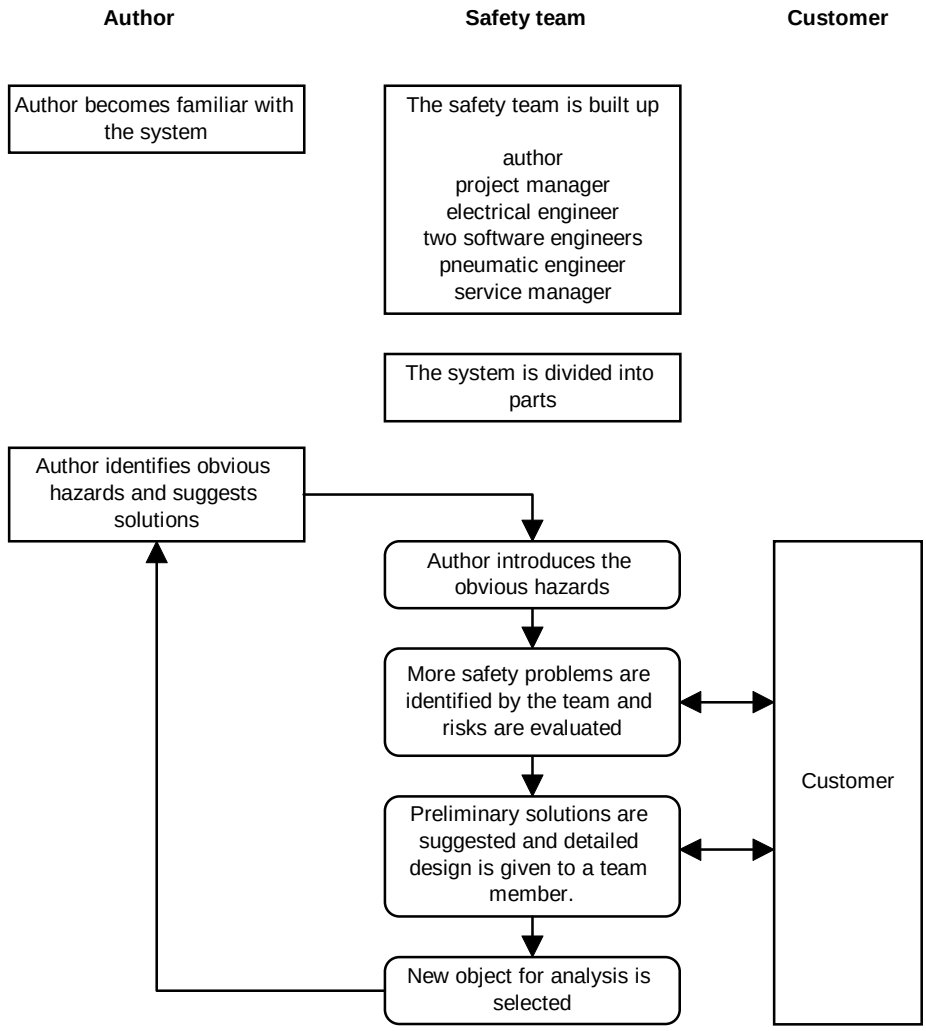

Figure 11. The safety team organisation.

The second package dealt with safety engineering. The target group was the designers. The aims of the second package were to learn the basics of isolation of energy source, emergency stop, safety devices and guards, safety distances, walkways and risk estimation. This kind of training supports the practical design work, making it possible to integrate the safety measures into the automation system simultaneously with the other features.

8.3.2 Risk estimation

The risks of the materials handling system were estimated according to EN 954-1 (1997). The method is developed to facilitate the design of safety-related parts of control systems. The risk estimation of the identified hazards and hazardous situations was carried out independently by the author, the project manager and the software engineer. A total of 256 risks of the system were estimated. The author divided the risks into five groups

– risks of moving parts
– risk of flying objects
– risks of falling of operator
– risks of temperature
– risk of fire.

The risk estimation (EN 954-1 1997) consists of the estimation of the severity of injuries caused by a hazard, the frequency of a hazardous situation or the exposure time to the hazard and the possibility of operators to avoid the accident (Figure 12).

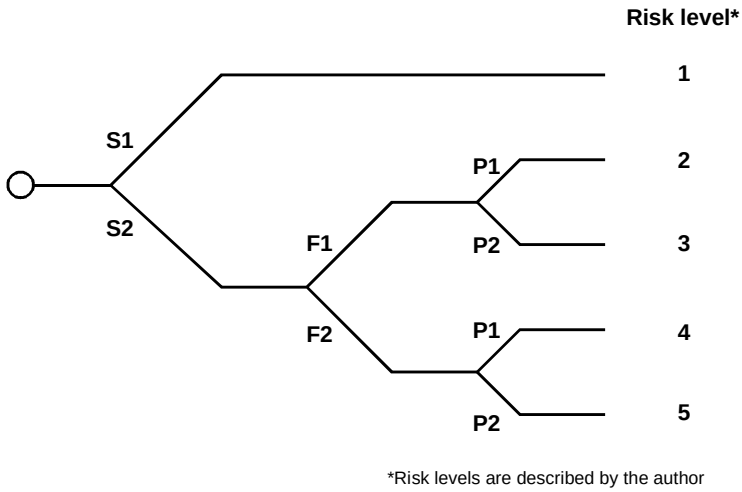

Figure 12. The risk estimation (EN 954-1 1997).

The severity of injuries can be slight injury (S1) or serious, normally irreversible, injury including death (S2). The frequency and/or the exposure time to the hazard can vary from seldom to quite often and/or the exposure time can be short (F1). Alternatively, the frequency and exposure can vary from frequent to continuous and/or the exposure time can be long (F2). The operator can avoid the hazard under specific conditions (P1) or the avoiding of the hazard can be scarcely possible (P2). In this case, the outcomes of the combinations of the severity, the frequency and the possibility to avoid the hazards are called risk levels.

The severity of injuries was estimated by according the value 1 to severity S1 and the value 2 to severity S2 (Table 11). The frequency and the possibility of operators to avoid the accident were estimated similarly.

Table 11. An example of the risk estimation.

Hazard	**Author**			**Project manager**			**Software engineer**		
	S	**F**	**P**	**S**	**F**	**P**	**S**	**F**	**P**
Moving part 1	1	1	2	1	1	2	2	2	1
Moving part 2	2	2	1	2	1	2	2	2	1
Falling 1	2	2	1	1	1	1	2	2	1
Falling 2	2	1	1	1	1	1	2	1	1
.									
.									
.									

The results of the risk estimation were crosstabulated. The differences in the risk estimations were evaluated by comparing the count values of estimations with the expected count values. In addition, the column percentages within the severity, frequency and possibility of operators to avoid the hazard were compared. Finally, the Pearson χ^2-test was carried out to evaluate the significance of the personal differences in the estimations.

8.4 Hazards of the materials handling system

The safety team met 7 times and the meetings lasted for 2 hours. A total of 79 manhours were spent on safety teamwork. In addition, the author spent approximately 40 manhours becoming familiar with the system and about 80 manhours carrying out the safety analysis. The safety team identified a total of 398 hazards and related hazardous situations, 70 of which were related to the operation of the system. Programming and adjustment accounted for 80 hazardous situations and maintenance for 78 hazardous situations. 85 hazardous situations were related to disturbance control and 85 hazards to cleaning.

The fast and possibly unexpected movements of the robots cause severe hazards in all operation tasks. The robots and the hot front panels can hit and burn the operators and crush the operator against surrounding structures, or the hot front panels can fly against the operators or surrounding structures. The access to hazardous areas and the hazards of flying front panels can be prevented by safety fences with interlocked gateways to the hazardous areas. Adequate clearances between the moving parts of the robots and the surrounding structures prevent the crushing. It is also important to apply special safety measures like reduced speed or incremental step-by-step movements if the operator has to carry out work tasks in the hazardous area.

The conveyor must be designed in a such way that the hazards caused by the chain drives and the nippoints between rolls, belts and structures are prevented. The typical hazardous situations are the cleaning of the conveyors and the unexpected start-ups that can cause crushing or falls.

In addition to the traditional hazards of automation, many special hazards are involved, such as hot glass, glass fragments, hot environment and glass particles in the air. The temperature of the glass is over 600 C^{O} and it emits heat to the environment and the structures causing thermal stress and burns. The front panel can break if it cools too fast and the cleaning of the sharp glass fragments can cause severe wounds. Heat can also cause failures in the control system.

The concurrent engineering approach led to several changes in previous safety measures, user instructions and training. In addition, usability and availability was improved by changes in the control system, walkways, service and

maintenance procedures and disturbance control procedures. A total of 94 design tasks for safety were started on the basis of the safety analysis. In addition, the essential health and safety requirements concerning instructions, markings and technical documentation were considered.

8.5 Risk estimation

The Pearson χ^2-test showed that the estimations of the severity of the injuries caused by the hazards differed significantly (χ^2=24.168, df =8, p=0.002). On the basis of the count values and the expected count values, it seems that the author overestimated and the project manager underestimated the severity of the injuries caused by the moving parts (Table 12). On the other hand, the author underestimated the injuries caused by the flying objects when the project manager and the software engineer considered the injuries more severe. In addition, the project manager estimated the severity of the injuries caused by the high temperature higher than the author and the software engineer. The difference is especially high if the percentages within the severity are compared.

The estimations of the frequency and the exposure times to hazards did not differ between the author, the project manager and the software engineer. The materials handling system is designed to work fully automatically. Therefore, the user does not need access to hazardous areas during the normal operation of the system and the frequency of the hazardous situations was considered to vary from seldom to quite often. The typical hazardous work tasks are disturbance control, maintenance and cleaning of the system. However, the situation changes if the reliability of the system is not as high as expected. In that case the frequency and the exposure times can increase radically.

Table 12. The estimations of the severity of the injuries.

Person		Moving parts	Flying objects	Falling of operator	High temperature	Fire
Author	Count	254	31	12	86	5
	Expected count	221.3	43.1	10.6	109.5	3.5
	% within severity	33.9%	21.2%	33.3%	23.2%	41.7%
Project manager	Count	258	62	12	169	4
	Expected count	288.0	56.1	13.8	142.5	4.6
	% within severity	34.4%	42.5%	33.3%	45.6%	33.3%
Software engineer	Count	238	53	12	116	3
	Expected count	240.7	46.9	11.6	119.1	3.9
	% within severity	31.7%	36.3%	33.3%	31.3%	25.0%

The estimations of the operator's possibility to avoid the hazard differed significantly (χ^2=13.636, df =8, p=0.092). According to the count values and the expected count values, the author underestimated and the project manager and the software engineer overestimated the operator's possibilities to avoid the hazards caused by the moving parts (Table 13). The author slightly overestimated the operator's possibilities to avoid the flying objects, but the software engineer doubted the operator's possibilities to avoid the hazards caused by the flying objects. The author also estimated the operator's actual possibilities to avoid the hazards caused by the high temperature higher than the project manager. The percentages within the column falling of operator indicates that the software engineer considered the operator's possibilities to avoid falling lower than did the author and the designer.

Table 13. The estimations of the operator's possibility to avoid the hazard.

Person		Moving parts	Flying objects	Falling of operator	High temperature	Fire
Author	Count	235	34	6	85	3
	Expected count	211.0	42.2	8.7	97.3	3.8
	% within the operator's possibility to avoid	42.3%	30.6%	26.1%	33.2%	30.0%
Project manager	Count	151	34	6	86	4
	Expected count	163.3	32.7	6.8	75.3	2.9
	% within the operator's possibility to avoid	27.2%	30.6%	26.1%	33.6%	40.0%
Software engineer	Count	169	43	11	85	3
	Expected count	180.7	36.1	7.5	83.4	3.3
	% within the operator's possibility to avoid	30.5%	38.7%	47.8%	33.2%	30.0%

8.6 Discussion

The manual handling of the hot front panels causes severe risks to a worker's health and safety. The risks caused by continuous exposure to thermal stress, glass particles in the air, high possibility of severe wounds caused by sharp glass fragments, injuries caused by explosion of cooling front panels and hot flying glass fragments can be removed or reduced by automating materials handling. The new automation, however, causes different risks that must be managed during the design, implementation and operation of the system. The risks of a well-designed automatic materials handling system are obviously lower than the risks of manual work.

The safety team identified hazards and implemented safety measures concurrently with other design objectives. The risk assessment identified hazards that were not realised in the early design stages and for which the designers would not have designed the necessary safety measures. The risk assessment also clarified the design requirements and the alternative safety measures to protect against the hazards.

The systematic safety design was started during completion of the overall layout of the system. Thus it was not possible to make radical changes to the layout of the robots and conveyors, but it was possible to change the position of safety fences, gateways and walkways. The systematic assessment of the hazards of the key modules of the layout helped the safety design team to select and design necessary safety measures.

The safety design on the basis of the risk assessment was more comprehensive than the design on the basis of the few obvious hazards that were identified at the beginning of the project. The safety teamwork also improved the quality of the safety measures, because it involved more designers being in a position to evaluate the benefits and drawbacks of the suggested safety measures.

The risk estimation was carried out according to EN 954-1 (1997). The risk estimation did not provide a clear quantitative answer concerning the acceptability of the risks. However, the risk estimation helped the design team to evaluate the importance of the different risks, providing qualitative aid for decision making. On the other hand, the results showed that the risk estimation yielded unreliable results when it was carried out by individuals. Especially the estimations concerning the severity of injuries and the possibilities of operators to avoid the hazards deviated significantly. Therefore, the joint judgement of a design team is needed when risks are estimated and evaluated. Thus, the risks must be estimated and evaluated and the safety measures must be designed by a team on the basis of concurrent engineering.

9. Case 4: Safety design of a trim cutting machine

9.1 Introduction

A small designing and manufacturing company had developed a new type of technology for trim cutting in papermills. On the basis of the new technology the company had built a prototype that was used to test the technology and collect experience on the practical functioning of the technology. The company also used the prototype to demonstrate the functioning of the machine for potential customers.

The new technology proved to be promising and customers showed interest in the machine. Hence, the company started to design the commercial version of the machine. The company was aware of the essential health and safety requirements of the machinery safety directive (Directive 98/37/EC). Therefore, the safety design was carried out during the design process.

The aims of the case were

- to fulfil the essential health and safety requirements of the trim cutting machine
- to evaluate the possibilities of a small company to carry out reliable risk assessment and a safety design process.

9.2 The trim cutting machine

The trim cutting machine is used in papermachines to cut the uneven edge of a paper web before a reel-up. The trim cutting machine is located to the side of the paper web. Machine control is typically integrated into the control system of the paper machine. This type of machine cuts the paper with a high-pressure water jet (Figure 13). The machine consists of pressure unit, cutting unit and air blast unit. The pressure unit generates high-pressure water which is brought to the cutting unit by the high-pressure hose. The cutting unit consists of moving carriage, cutting head, cutting table and vacuuming nozzle, which vacuums the cut trim to the pulper.

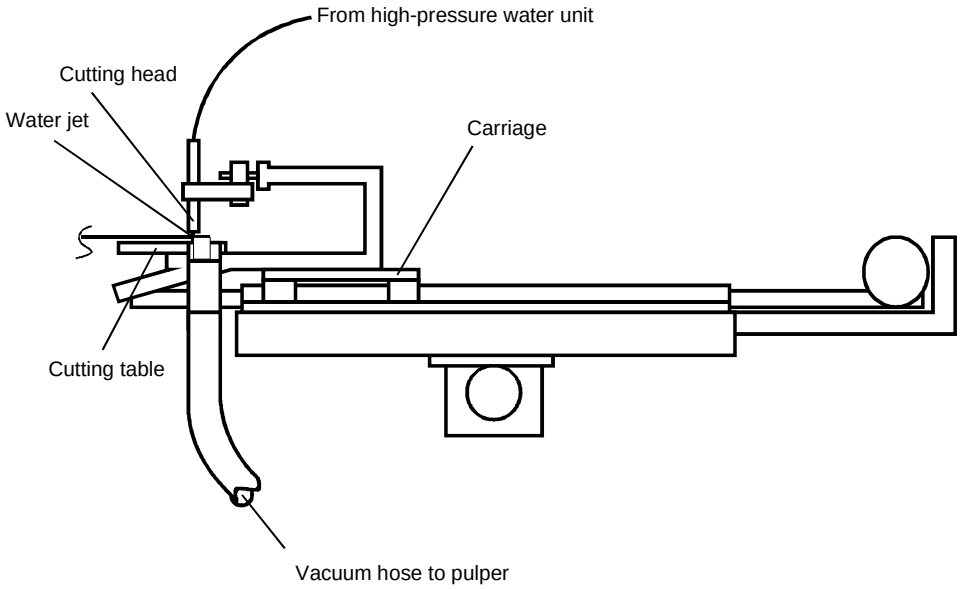

Figure 13. The trim cutting machine.

9.3 Method

The functioning and reliability of the high-pressure water system was designed and tested in 1998. At the same time, systematic safety design was started. The first prototype was tested in papermills at the end of 1998 and the first machine was delivered to a papermill in 1999. The designer had strong experience in designing different kinds of auxiliary machines for papermills.

The trim cutting machine was analysed by the designer of the machine and the author together with the users of the machine. The safety design process started with the risk assessment of the prototype and comparison between the prototype and the essential health and safety requirements of the machinery safety directive (Directive 98/37/EC). In addition, the designer and the author visited a papermill and had discussions with the potential users. On the basis of the risk assessment, the design of the safety measures was started. The final safety measures were designed on the basis of the discussions with customers.

The determination of limits and functions of the machine and users was carried out by the designer and the author. The designer described the machine, the environment and the tasks of operators to the author, who documented the results. A total of 14 manhours were used in the determination phase.

The hazards and hazardous situations of the machine were identified by the designer and the author. The author wanted to evaluate the reliability of the hazard identification and therefore the designer and the author carried out the hazard identification separately. After the separate hazard identification, the designer and the author compared the results and completed the analysis. A total of 10 manhours were spent on the hazard identification.

The risks of the hazardous situations related to the prototype were estimated and evaluated according to EN 954-1 (1997) by the designer and the author. The results were applied to identify the most important risks. The designer and the author used 6 manhours on the risk estimation and evaluation. The prevention of the most important hazards and hazardous situations was added to the safety design specification. In addition, the technical requirements of the machinery safety directive that were not related to the hazards but were relevant for the trim cutting machine were added to the safety design specification. The preparation of the first version of the safety design specification required 8 manhours of work.

The author and the designer visited a papermill in order to verify the safety design specification. The installation environment of the prototype was reviewed and the users were interviewed about their experience with the machine. The results were added to the safety design specification.

The design of safety measures was carried out on the basis of the safety design specification. The basic safety measures were designed for the general configuration of the machine. It was understood that the safety measures may differ on the basis of the configurations.

The final safety design was carried out for the machine that was delivered to the first customer. The configuration was simpler than the general configuration and some of the hazards related to the general configuration did not exist. The special requirements related to the installation and operating site were analysed

by the designer, the author and a new mechanical designer joined the project, together with a group of users and managers from the papermill. The group consisted of two users, an occupational safety official, a shifter, an occupational safety manager and a hydraulic engineer. In addition, the trim cutting machine was connected to the control system of the papermachine by the customer's automation unit. Therefore, the designers and the members of the customer's automation unit went through the safety functions of the trim cutting machine.

9.4 Hazards of the trim cutting machine

A total of 75 hazards and related hazardous situations were identified in the first hazard identification carried out by the designer and the author. The cutting process is based on high water pressure. Therefore, the hydraulic energy and pneumatic energy play an important role in the safety of the system. The energies caused 33% of all hazards. Risks caused by the energy were also considered high. Two of the hazardous situations were considered to belong to the highest risk category 5 (Table 14).

An uncontrolled water jet can lead to amputations, severe wounds and possibly death in the cases of faulty installation or breakage of the cutting head. The water jet is also difficult to see and it is difficult the users to avoid the hazard even in the case of normal use. Special attention is paid to avoiding the hazards of the water jet. For example, leakage of the water system stops the machine automatically. In addition a chain prevents free swinging of the hose and cutting head if the fastening of the cutting head fails. The distance between the cutting head and the cutting table is small enough to prevent the user from putting his/her finger under the water jet and the fastening of the cutting head is secured by two independent mechanisms.

Table 14. The number of different risks (EN 954-1 1997) of the trim cutting machine.

Hazards	Number of different risks of the machine					Number of negligible hazards	Number of hazards	%
	Risk level (Figure 12)	1	2	3	4	5			
Energy		4	8	8		2	3	25	33
Moving parts, power transmission and machine actuators		6	2	8			2	18	24
Work environment		6	4	3	1		2	16	21
Materials and products		5	1	1			1	8	11
Lifting and materials handling			3	2			1	6	8
Access to operating area			2					2	3
Total		21	20	22	1	2	9	75	100

The papermachine can be equipped with threading rope at the side of the paper web. The cutting head must be moved over the threading rope and therefore the water jet must be stopped and the cutting head must be lifted. The water jet must not start in any circumstances when the cutting head is lifted, because the water jet can cut the threading rope or cause injury to the operator. In addition, the water jet must not start unexpectedly during maintenance of the cutting head. Therefore, the isolation of the energy source must affect both the high-pressure unit and the cutting unit.

Moving parts of the cutting machine together with machine actuators caused 24% of hazards. Most of the hazards were related to movements of the cutting carriage. Crushing between the carriage and the surrounding structures can be prevented by sufficient clearances. The speed of the carriage is slow, making it possible to avoid the hazard. However, crushing hazards are closely related to the place of installation and they must be considered case by case.

The trim cutting machine is located in a papermill. The work environment caused 21% of all hazards. Hazards are related for example to noise, insufficient

lighting and possible fire. The environment can also be wet and dirty, which causes additional need for cleaning the machine. The threading rope can also become entangled between paper rolls and fly against the trim cutting machine and break the machine. To prevent the hazard, heavy and rigid guards are needed.

Hydraulic and pneumatic oil are the material-related hazard sources of the trim cutting machine. In addition, different kinds of materials are used in the paper making process that are not known to the manufacturer of the cutting machine. A total of 11% of identified hazards were related to materials.

Lifting and materials handling caused 8% of all hazards. Typical hazardous situations exist during the transportation, installation and maintenance of the machine. Access to machine caused 3% of all hazards. The users are exposed to the hazards of the rolls of the paper machine, the paper track and unexpected movements of other auxiliary machines during the cleaning, maintenance and manual operation of the trim cutting machine. Special attention must be paid to the design of walkways and working platforms that are needed to access the trim cutting machine.

9.5 Reliability of the hazard identification

The reliability of the hazard identification was tested in order to evaluate the company's ability to carry out a safety design process on the basis of risk assessment. The author and the designer identified hazards of the trim cutting machine and the related hazardous situations independently. The numbers of hazards and the hazardous situations identified by the designer and the author were compared and the severity of the hazards that were not identified by the designer or the author were evaluated.

The designer identified 35% of 75 hazards and hazardous situations, while the author identified 92%. The designer identified 40% and the author identified 96% of hazards and hazardous situations caused by energy. Moving parts caused 16 hazards and hazardous situations of which 19% were identified by the designer and 94% by the author. A total of 31% of the hazards associated with the work environment were found by the designer and 94% by the author.

The author identified 88% and the designer 13% of the materials and products related hazards and hazardous situations. 83% of lifting and materials handling hazards were identified by the author and 50% by the designer. The author and the designer identified two hazards associated with the machine actuators. The author identified one hazard that was related to operation area and the designer identified two hazards.

The most dangerous risks at risk level 5 (Table 15) were identified by the designer and the author. The risk at risk level 4 was identified only by the author. The designer and the author found 5 identical risks that belong to risk level 3. In addition, the designer found one risk that was not noted by the author. The author identified 16 risks at risk level 3 that were not noted by the designer (Table 15).

Table 15. Number of risks identified by the designer and the author.

Risk level (See Table 14)	**Number of risks**	**Number of risks identified by the designer**	**Number of risks identified by the author**	**Number of identical findings**
Negligible hazard	9	2	8	1
1	21	3	20	2
2	20	13	17	10
3	22	6	21	5
4	1	0	1	0
5	2	2	2	2
Total	75	26	69	20

Both the designer and the author identified 10 risks at risk level 2. In addition, the designer identified three risks and the author seven risks that were not noted by the other analyst. The author and the designer made two identical identifications of risks in risk category 1. The designer found one risk that was identified by the author and the author found 18 risks that were not identified by the designer. Finally, both analysts identified one same risk that was negligible. In addition, the author found seven negligible risks and the designer one (Table 15).

9.6 Discussion

The safety design process improved the safety of the trim cutting machine. New hazards were identified and safety measures to protect against them were designed and implemented. The systematic analysis and safety design of the basic configuration of the trim cutting machine made the safety design of the actual customer configuration easy.

Both the designer and the author identified the most dangerous hazards well, but the designer missed one critical hazardous situation at risk level 4 and 16 risks at risk level 3 (Table 15). The main difference was that the author paid more attention to details and possible hazardous situations. The designer identified hazards, but he did not identify hazardous situations and accident scenarios. In addition, the author used more effectively the results of the determination phase than the designer. Hence, the design process would have lacked essential safety information without the additional help in safety design.

The results suggest that small companies with limited resources may have difficulties in carrying out an adequate risk assessment. Small companies may also lack sufficient skills in safety design. The design of a new type of machine requires an analytical approach to safety because new hazards are involved and previous experience is limited. Many practical designers use a solution-oriented approach to design (Cross 1989, p. 17) and analytical and problem-oriented methods are not used. Safety design on the basis of risk assessment is an analytical and problem-oriented approach. The differences in the approaches can cause difficulties when implementing safety design in the practical design process. Therefore, the integration of the safety design in a company's design practice requires either a more systematic approach to design or more solution-oriented safety considerations. However, the systematic and analytical approach has proved to lead to more optimal solutions (Günther & Ehrlenspiel 1999) and in the case of safety it is preferable.

10. Discussion

10.1 Improvements in safety

The risk assessments identified over 600 hazards and hazardous situations and more than 200 safety design tasks were started. The companies would not have carried out the systematic safety design processes without the obligations of the machinery safety directive (Directive 98/37/EC). Hence, the directive had a positive effect on the quality of the design process. At the same time, the risks of machines were reduced as the risk-reduction measures made them safer. However, the real accident data was not applied to evaluate the significance of the safety improvements.

Most of the safety-related design tasks were related to the user instructions and the structure of the machines. The multidisciplinary safety teamwork also created a natural forum for discussing the other problems related to machines. The safety design process has a positive effect on the usability and availability of machines by clarifying user work tasks and by improving maintenance and disturbance-control procedures.

10.2 Weaknesses of the machinery safety directive

The machinery safety directive (Directive 98/37/EC) sets out specific requirements for the safety measures and all of the requirements cannot be fulfilled on the basis of hazard identification. Therefore, the essential health and safety requirements of the machinery safety directive must be gone through in addition to hazard identification and risk evaluation.

The machinery safety directive (Directive 98/37/EC) obliges the machine manufacturer to assess the hazards of the machine to be designed and to fulfil the mandatory health and safety requirements on the basis of this assessment. However, the directive and the related standards do not provide sufficient aid for the manufacturer to evaluate the adequacy of the safety measures. A problem arises when all the safety objectives cannot be fulfilled and the acceptability of remaining risks must be evaluated.

The machinery safety directive (Directive 98/37/EC) mixes hazards and the safety goals in a confusing way. For example, the essential requirement: “materials must not endanger persons’ safety or health“, is actually the safety goal and the actual safety problem is the hazard related to the material. According to the initial idea of the machinery safety directive (Directive 89/392/EEC Annex 1, Preliminary observations) the essential health and safety requirements should have been grouped according to the hazards which they cover. However, the current directive (Directive 98/37/EC) or the proposal for a new draft of the directive on machinery (Proposal for... 1998) does not fulfil the idea.

Therefore, the new machinery safety directive must be structured in such a way that it first indicates the hazard and then the related safety goal. In addition, the directive should clearly show the appropriate safety measure against the hazard. If this is not possible, then the directive should indicate the means or procedures for fulfilling the safety goal. In addition, the directive should describe the safety measures that are not related to hazards but to functions and the structure of the machine, work tasks and user information.

10.3 Risk assessment

The main benefit of the systematic risk assessment was the clarification of the safety design requirements. The systematic assessment of the risks of the machine provided wider and deeper knowledge about the different safety requirements of the machine and benefits and drawbacks of the alternative design solutions. The hazards of the machine were identified mainly on the basis of the hazard lists of EN 292-1 (1992) and EN 1050 (1997) together with the information from the determination of the limits and functions of the machine, users and environment (Appendix 1).

Despite the fact that the created number of hazards were identified in risk assessments, it seems that some people are able to handle both the hazards and the possible accident scenarios, while others identify hazards but do not consider the possible accidents. Therefore, during the design process they lack the information that connects the hazards to the actual work tasks. Therefore,

the use of the machine and user instructions are considered at the end of the design process and the possibilities of safety design are restricted.

The identified risks of the machines were estimated according to the EN 954-1 (1997) or the previous draft of the standard. The method is based on the EN 1050 (1997), but it is simplified. The standard aims to facilitate selection of components for safety-critical control systems. The standard is not a machine risk estimation method and therefore the results cannot be applied to evaluate acceptability of risks. However, the method can be applied to show the difference between different kinds of hazardous situations and possible accidents. Thus, it can be applied to prioritise the hazards. In addition, it proved to be a good tool for educational purposes. The method helps designers to understand the concept of risk. Hence, the designers were able to evaluate the hazardous situations on the basis of same criteria and to make decisions about the importance of the further safety design. Unfortunately, many problems are related to the reliability of the risk estimation according to EN 954-1 (1997). Case 3 showed that the most difficult aspects to consider in the risk estimation were the severity of the injuries and the possibility of users to avoid the accidents. These results illustrated the importance of carrying out the risk estimation together with another designer instead of forming individual judgements.

10.4 Integrating safety into the general design process

The approach fulfilling European machine safety requirements was developed on the basis of general theories of safety, the iterative process to achieve safety (EN 1050 1997) and the essential health and safety requirements of the machinery safety directive (Directive 98/37/EC). The safety was integrated into the design process described in VDI 2221 (1993). Therefore, it was possible to apply the approach to different kinds of machines, in the different branches of industry and in different kinds of design situations.

During its development the approach fulfilling European safety requirements was tested from different points of view. The approach was safety conscious (Koivisto 1996, p. 40) and the advanced safety level (Kuivanen 1995, p. 58) was applied in design. The essential requirements of the law were fulfilled taking

into account simple demands of the production and production system. The approach concentrated on safety and lacked comprehensive ergonomic considerations.

Cases 1 and 2 were related to the redesign of existing machines. Case 4 was related to the safety design of a prototype and the design process was similar to redesign. Case 1 was the food mixing machine, case 2 was the colour tinting machine and case 4 was the trim cutting machine. The design problem was clearly focused on the safety requirements. The risk assessments were easy to carry out by observing the existing machines and work tasks. On the other hand, the design tasks were highly constrained in cases 1 and 2. The basic solution principle of the machine functions could not be changed and therefore the solution principles for the risk-reduction measures were mainly limited to the user instructions and safety devices. In case 4 the basic structure of the machine was already decided and fixed, but the design of the safety measures was not as constrained as in cases 1 and 2.

Case 3 was related to the design of a large automatic materials handling system. The safety design was started after the preliminary layouts of the system were designed and partly fixed. The risk assessment was carried out on the basis of drawings by the safety design team. The multidisciplinary teamwork and the less constrained design task compared with cases 1 and 2 made it possible to completely remove certain hazards and to make changes in the layout of the system. Thus, it was easier to design the solution principles for the safety measures. The teamwork made it also possible to affect other safety-related properties of the system, like usability and maintainability.

The development process of the approach fulfilling European safety requirements was mainly directed by the author. Therefore, the result corresponds to the needs of a consulting safety expert. The experience gained showed that first safety analysis is difficult to carry out and the practical application of the approach requires training. Safety training and education concerning the new European safety requirements were given in all cases. However, the case studies were carried out as single analyses. The scopes of the cases did not cover the organisational aspects that would have been needed to implement the approach to the design organisation. Therefore the implementation of the approach was not fully satisfactory.

10.5 Need for further studies

On the basis of this study, two important problems should be investigated. The real effects of the machinery safety directive on the accident rates of different kinds of machines is not known. This problem must be studied in order to evaluate the importance of the machinery safety directive on safety in real life. The actual effects should be known when evaluating the importance of the proposal for a new draft of the directive on machinery (Proposal for… 1998).

The machinery safety directive (Directive 98/37/EC) or the related standards provide insufficient aid for the manufacturer to evaluate the adequacy of the safety measures. Therefore, practical methods for evaluating the acceptability of risks are needed.

In addition, the integration of the essential health and safety requirements into the different design strategies must be studied. In this study, the integration of the requirements into systematic and analytical design strategy was studied, but safety design in a short design process under high time pressure (Günther & Ehrlenspiel 1999) needs to be studied.

11. Conclusions

The main benefit of the approach fulfilling the European safety requirements was the clarification of the safety design requirements. The hazards of a machine and possible losses cause design problems that must be solved during the design process. Hence, risk assessment and the design for risk-reduction measures can be carried out simultaneously with other design objectives in all design stages by multidisciplinary design teams.

The machinery safety directive (Directive 98/37/EC) sets out the essential health and safety requirements and requires the manufacturer to assess the hazards of a machine. However, the directive and the related standards do not provide sufficient aid for the manufacturer to evaluate the adequacy of the safety measures and the acceptability of the remaining risks. Therefore, practical methods for evaluating the acceptability of risks are needed.

The machinery safety directive (Directive 98/37/EC) mixes hazards and the safety goals in a confusing way. The essential health and safety requirements should be grouped according to the hazards which they cover. However, the proposal for a new draft of the directive on machinery (Proposal for... 1998) does not fulfil the idea. Therefore, the new machinery safety directive (Proposal for... 1998) must be structured in such a way, that it first indicates the hazard and then the related safety goal. After that, the directive must clearly show the appropriate safety measure against the hazard. If it is not possible to describe the safety measure, then the directive must describe the design and the evaluation procedures that can be applied to assess the fulfilment of the safety goal. In addition, the directive should describe the safety measures that are not related to hazards but to functions and the structure of the machine, work tasks and user information.

The harmonised C-level standards do not necessarily cover all the essential safety problems related to the machine to be designed. Therefore, in addition to hazards covered by the C-level standards, special attention should be paid to identifying the accident scenarious caused by the working environment and the actual work tasks. Therefore, it is recommended to carry out comprehensive risk assessment even if the C-level standard provides a machine-specific list of hazards and related safety measures.

Risk estimation according to EN 954-1 (1997) was unreliable. The individual judgements about the severity of the consequences and about the possibility of the user to avoid accident varied drastically. Therefore, it is always recommended that the risk estimation should be carried out by a team. On the other hand, it is not self-evident that designers are able to carry out the necessary risk assessments. Therefore, sufficient training in safety design is needed to create the necessary safety design capabilities.

References

Aaltonen, M., Uusi-Rauva, E., Saari, J., Antti-Poika, M., Räsänen, T. & Vinni, K. 1996. The accident consequence tree method and its application by real-time data collection in the Finnish furniture industry. Safety Science, Vol. 23, pp. 11–26.

Abbot, H. 1987. Safer by design: the management of product design risks under strict liability. London: The Design Council. 208 p.

Akao, Y. 1988. Quality Function Deployment: Integrating Customer Requirements in Product Design. Portland: Productivity Press. 369 p.

Badke-Schaub, P. & Frankenberger, E. 1999. Analysis of design projects. Design Studies, Vol. 20, pp. 465–479.

Ballard, G. 1993. Societal risk - progress since farmer. Reliability Engineering & System Safety, Vol. 39, pp. 123–127.

Barnett, R. & Brickman, B. 1986. Safety hierarchy. Journal of Safety Research, Vol. 17, pp. 49–55.

Behesti, R. 1993. Design decisions and uncertainty. Design Studies, Vol. 14, pp. 85–95.

Beitz, W. 1997. Quality through customer integration and systematic design. In: Riitahuhta, A. (ed.). Proceedings of the 11th International Conference on Engineering Design, Tampere, Finland, 19–21 August, 1997. Tampere: Tampere University of Technology, Vol. 1, pp. 281–284.

Broberg, O. 1997. Integrating ergonomics into the product development process. International Journal of Industrial Ergonomics, Vol. 19, pp. 317–327.

Brown, S. 1995. What Customers Value Most. Toronto: John Wiley & Sons. 304 p.

BS 8800. 1996. Guide to occupational health and safety management system. [London]: British Standards Institution BSI. 40 p.

Busby, J. 1997. The neglect of feedback in engineering design organisations. Design Studies, Vol. 19, pp. 103–117.

CEN/TC153/HN124E. 1993. Food processing machinery. Safety and hygiene requirements. Basic concepts - Part 2: Hygiene requirements. European Committee for Standardization. 27 p.

CEN/TC153/SN1. 1992. Food processing machinery. Safety and hygiene requirements. Basic concepts. Part 1: Safety requirements. European Committee for Standardization. 33 p.

CEN/TC153/WG2/N5.4E. 1991. Meat processing machinery - Mixers and mixing machines - Safety and hygiene requirements. European Committee for Standardization. 21 p.

Constable, G. 1992. Ten ways to mismanage product design. Engineering Management Journal, Vol. 2, pp. 131–136.

Cooke, J., McMahon, C. & North, M. 1997. In: Riitahuhta, A. (ed.). Proceedings of the 11th International Conference on Engineering Design, Tampere, Finland, 19–21 August, 1997. Tampere: Tampere University of Technology, Vol. 3, pp. 125–130.

Cross, N. 1989. Engineering Design Methods. Chichester: John Wiley & Sons. 159 p.

Crossland, R., Williams, J. & McMahon, C. 1995. An object-oriented design model incorporating uncertainty for early risk assessment. In: Hubka, (ed.). Proceedings of the 10th International Conference on Engineering Design, Prague, Czech, 22–24 August, 1995. Zürich: Heurista. Pp. 1555–1556.

Culley, S., Boston, O. & McMahon, C. 1999. Suppliers in new product development: Their information and integration. Journal of Engineering Design, Vol. 10, pp. 59–75.

Culvenor, J. & Dennis, E. 1997. Finding occupational injury solutions: The impact of training in creative thinking. Safety Science, Vol. 25, pp. 187–205.

Dickinson, C. 1995. Proposed manual handling International and European standards. Applied Ergonomics, Vol. 26, pp. 265–270.

Directive 89/392/EEC. 1989. Council directive on the approximation of the laws of the Member States relating to machinery (89/392/EEC). Official Journal of the European communities, No. L 183. Pp. 9–32.

Directive 98/37/EC. 1998. Directive 98/37/EC of the European Parliament and of the Council of 22 June 1998 on the approximation of the laws of the Member States relating to machinery, Official Journal, L 207. Pp. 1–46.

Drury, C. 1997. Ergonomics and the quality movement. Ergonomics, Vol. 40, pp. 249–264.

Dym, C. & Levitt, R. 1991. Knowledge-Based Systems in Engineering. New York: McGraw-Hill. 404 p.

Ekelenburg, H., Hoogerkamp, P. & Hopmans, L. 1995. A Practical Guide to the Machinery Directive. London: Mechanical Engineering Publications Limited. 320 p.

Eklund, J. 1997. Ergonomics, quality and continuous improvement - conceptual and empirical relationships in industrial context. Ergonomics, Vol. 40, pp. 982– 1001.

EN 292-1. 1992. Safety of Machinery. Basic concepts, general principles for design. Part 1: Basic terminology, methodology. Helsinki: Suomen standardisoimisliitto. 37 p.

EN 414. 1992. Safety of machinery. Rules for the drafting and presentation of safety standards. Helsinki: Suomen standardisoimisliitto. 30 p.

EN 418. 1993. Safety of machinery. Emergency stop equipment, functional aspects. Principles for design. Helsinki: Suomen standardisoimisliitto. 14 p.

EN 954-1. 1997. Safety of machinery. Safety-related parts of control systems. Part 1: General principles for design. Helsinki: Suomen standardisoimisliitto. 65 p.

EN 1050. 1997. Safety of machinery. Principles for risk assessment. Helsinki: Suomen standardisoimisliitto. 42 p.

EN 60204-1. 1998. Safety of machinery. Electrical equipment of machines. Part 1: General requirements. Helsinki: Suomen standardisoimisliitto. 181 p.

Gause, D. & Weinberg, G. 1989. Exploring Requirements: Quality Before Design. New York: Dorset House Publishing. 299 p.

Gauthier, F. & Charron, F. 1995. Design for health and safety: a simultaneous engineering approach. In: Hubka, V. (ed.). Proceedings of 10th International conference on Engineering Design. Prague, Czech, 22–24 August, 1995. Zürich: Heurista. Pp. 891–896.

Günther, J. & Ehrlenspiel, K. 1999. Comparing designers from practice and designers with systematic design education. Design Studies, Vol. 20, pp. 439– 451.

Hale, A., DeLoor, M., van Drimmelen, D. & Huppes, G. 1990. Safety standards, risk analysis and decision making: Implications of some recent European legislation and standards, Journal of Occupational Accidents, Vol. 13, pp. 213– 231.

Hale, A., Heming, B., Carthey, J. & Kirwan, B. 1997. Modelling of safety management systems. Safety Science, Vol. 26, pp. 121–140.

Hale, A. & Swuste, P. 1998. Safety rules: procedural freedom or action constraint? Safety Science, Vol. 29, pp. 163–177.

Hales, C. 1995. Five fatal design. In: Hubka, V. (ed.). Proceedings of 10th International conference on Engineering Design. Praha, Czech, 22–24 August, 1995. Zürich: Heurista. Pp. 662–667.

Harms-Ringdahl, L. 1987. Safety analysis in design - Evaluation of a case study. Accident Analysis & Prevention, Vol. 19, pp. 305– 317.

Haslegrave, C. & Holmes, K. 1994. Integrating ergonomics and engineering in the technical design process. Applied Ergonomics, Vol. 25, pp. 211–220.

Heinonen, J. 1994. Model of Customer Oriented Product Development Systematics - and Its Testing in Petrochemical Industry. Tampere: Tampere University of Technology. 186 p. + app. 14 p.

Holts, K. 1989. Does the engineer forget the user. Design Studies, Vol. 10, pp. 163–168.

Hubka, V. & Eder, E. 1988. Theory of Technical Systems: A Total Concept Theory for Engineering Design. Berlin: Springer-Verlag. 275 p.

Höhne, G. 1997. Design optimisation by decision-making during the conceptual design phase. In: Riitahuhta, A. (ed.). Proceedings of the 11th International Conference on Engineering Design, Tampere, Finland, 19–21 August, 1997. Tampere: Tampere University of Technology, Vol. 3, pp. 169–174.

IEC 300-3-9. 1995. Dependability management. Part 3: Application guide - Section 9: Risk analysis of technological systems. Genève: International Electrotechnical Commission. 67 p.

Jardine, C. & Hrudey, S. 1997. Mixed messages in risk communication. Risk Analysis, Vol. 17, pp. 489–498.

Johnson, L. 1990. Quality: How to meet customer demands in a process from design to disposal. Journal of Occupational Accidents, Vol. 13, pp. 167–170.

Kivistö-Rahnasto, J. 1997. Design for safety by concurrent engineering. In: Fallon, E., Hogan, M., Bannon, L. & McCarthy, J. (ed.). Proceedings of the First International Conference on Allocation of Functions, Galway, Ireland, 1–3 October, 1997. Louisville: IEA Press, Vol. 2, pp. 129–132.

Kivistö-Rahnasto, J. & Mattila, M. 1995. Integration of information on safety standards in machine design. In: Hubka, V. (ed.). Proceedings of 10th International conference on Engineering Design. Prague, Czech, 22–24 August, 1995. Zürich: Heurista. Pp. 958–963.

Kjellén, U. & Sklet, S. 1995. Integrating analyses of the risk of occupational accidents into the design process. Part I: A review of types of acceptance criteria and risk analysis methods. Safety Science, Vol. 18, pp. 215–227.

Koivisto, R. 1996. Safety-Conscious Process Design. Espoo: VTT. 79 p. + app. 67 p. (VTT Publications: 264.)

Kroemer, K. & Grandjean, E. 1997. Fitting the Task to the Human. A Textbook of Occupational Ergonomics. London: Tayler & Francis. 416 p.

Kuivanen, R. 1995. Methodology for simultaneous robot system safety design. Espoo: VTT. 142 p. + app. 13 p. (VTT Publications: 219.)

Kuusela, J. 1998. Työympäristön tuottavuusvaikutukset [Productivity effects of working environment]. Tampere: Tampere University of Technology, Lictech, thesis. 103 p. + app. 29 p. (In Finnish)

Lowrance, W. 1976. Of Acceptable Risk: Science and the Determination of safety. Los Altos: William Kaufman. 180 p.

Lowrance, W. 1980. The Nature of Risk. Societal Risk Assessment: How Safe is Safe Enough?. In: Schwing, R. & Albers, W. (ed.). Societal Risk Assessment: How Safe Is Safe Enough? New York: Plenum Press. Pp. 5–17.

Luczak, H. 1998. Ethics and responsibilities in ergonomics. In: Scott, P., Bridger, R. & Charteris, J. (ed.). Global Ergonomics. Proceedings of the Ergonomics Conference, Cape Town, South Africa, 9–11 September, 1998. Oxford: Elsevier. Pp. 809–814.

Main, B. & Ward, A. 1992. What do design engineers really know about safety? Mechanical Engineering, Vol. 114, pp. 44–51.

Martin, M. & Schinzinger, R. 1996. Ethics in Engineering. 3.ed. New York: McGraw-Hill. 439 p.

Mattila, M., Tallberg, T., Vannas, V. & Kivistö-Rahnasto, J. 1995. Fatalities at Advanced Machines and Dangerous Incidents at FMS Implementations. The International Journal of Human Factors in Manufacturing, Vol. 5, pp. 237–250.

Montreuil, S. 1996. Ergonomics training for managers, employees and designers involved in the design and erganization of work systems. Safety Science, Vol. 23, pp. 97–106.

Nijhuis, K. & Roozenburg, N. 1997. Evaluation the use of product design specifications in Dutch product development practice. In: Riitahuhta, A. (ed.). Proceedings of the 11th International Conference on Engineering Design, Tampere, Finland, 19–21 August, 1997. Tampere: Tampere University of Technology, Vol. 2, pp. 281–284.

Pahl, G. & Badke-Schaub, P. 1999. Résumé of 12 years interdisciplinary empirical studies of engineering design in Germany. Design Studies, Vol. 20, pp. 481–494.

Pahl, G. & Beitz, W. 1996. Engineering Design. A Systematic Approach. Berlin: Springer-Verlag. 544 p.

Patwardhan, A., Kulkarni, R. & Nicod, J. 1990. Residual risk and its distribution in the pr42oject life cycle. Journal of Occupational Accidents, Vol. 13, pp. 79– 92.

prEN 13570. 1999. Food Processing Machinery. Mixers and Mixing Machines. Safety and Hygiene Requirements. European Committee for Standardization. 41 p.

Proposal for… 1998. Proposal for a new draft of the directive on machinery. EN-III/4101/97 rev. 3, 5.10.1998. 64 p.

Rahimi, M. 1995. Merging strategic safety, health and environment into total quality management. International Journal of Industrial Ergonomics, Vol. 16, pp. 83–94.

Reason, J. 1997. Managing the Risks of Organizational Accidents. Aldershot: Ashgate. 252 p.

Reunanen, M. 1993. Systematic safety consideration in product design. Espoo: VTT. 124 p. +app. 8p. (VTT Publications: 145.)

Roland, H. & Moriarty, B. 1983. System Safety Engineering and Management. New York: John Wiley & Sons. 339 p.

Roozenburg, N. & Eekels, J. 1995. Product Design: Fundamentals and Methods. Chichester: John Wiley & Sons. 408 p.

Roseman, M. & Gero, J. 1998. Purpose and function in design: from the socio-cultural to the techno-physical. Design Studies, Vol. 19, pp. 161–186.

Rouhiainen, V. 1993. Importance of the quality management of safety analysis. Reliability Engineering and System Safety, Vol. 40, pp. 5–16.

Rowe, W. 1977. An Anatomy of Risk. New York: John Willey & Sons. 488 p.

Rowe, W. 1980. Risk assessment approaches and methods. In: Condrad, J. (ed.). Society, Technology and Risk Assessment. London: Academic Press. Pp. 3–29.

Sadgrove, K. 1996. The Complete Guide to Business Risk Management. Aldershot: Gower. 224 p.

Sanders, M. & McCormick, E. 1993. Human Factors in Engineering and Design. 7.ed. New York: McGraw-Hill. 790 p.

Shaub, K. & Landau, K. 1998. The EU machinery directive as a source for a new ergonomic tool box for preventive health care and ergonomic workplace and product design. In: Scott, P., Bridger, R. & Charteris, J. (ed.). Global Ergonomics. Proceedings of the Ergonomics Conference, Cape Town, South Africa, 9–11 September, 1998. Oxford: Elsevier. Pp. 219–224.

Schön, G. 1993. Grundkonzept der Sicherheitstechnik. Safety Science, Vol. 16, pp. 343–358.

Smyth, L. 1997. Conceptualising designer-user-customer interfaces as the management of positive and negative feedback loops. In: Fallon, E., Hogan, M.,

Bannon, L. & McCarthy, J. (ed.). Proceedings of the First International Conference on Allocation of Functions, Galway, Ireland, 1–3 October, 1997. Louisville: IEA Press, Vol. 2, pp. 47–55.

Stewart, T. 1995. Ergonomics standards concerning human-system interaction. Applied Ergonomics,Vol. 26, pp. 271–274.

Stoop, J. 1990. Safety and the Design Process. Delft: Technische Universiteit Delft. 124 p.

Suh, N. 1990. The Principles of Design. New York: Oxford University Press. 401 p.

Suokas, J. 1993. Evaluation of the effect of safety regulations. Case studies on press and conveyor regulations. Safety Science, Vol. 16, pp. 307–324.

The New Approach... 1994. The New Approach. Legislation and standards on the free movement of goods in Europe. Brussels: European Committee for Standardization. 208 p.

Thomson, J. 1987. Engineering Safety Assessment: An introduction. Longman Scientific & Technical. 221 p.

Tiusanen, R., Hietikko, M. & Kivipuro, M. 1994. Ohjelmoitavan elektroniikan turvallisuuden arvioiminen [The safety evaluation of programmable electronics]. Espoo: VTT. 44 p. + app. 4 p. (VTT Research notes 1596.) (In Finnish)

Ullman, D. 1997. The Mechanical Design Process. [New York]: McGraw-Hill. 340 p.

Ulrich, K. & Eppinger, S. 1995. Product Design and Development. [New York]: McGraw-Hill. 289 p.

Van Aken, D. 1997. Consumer products: Hazard analysis, standardization and (re)design. Safety Science, Vol. 26, pp. 87–94.

VDI 2221. 1993. Methodik zum Entwickeln und Konstruieren technischer Systeme und Produkte [Systematic Approach to the Design of Technical Systems and Products]. Düsseldorf: Verein Deutcher Ingenieure. 44 p.

Weth, R. 1999. Design instinct? - the development of individual strategies. Design Studies, Vol. 20, pp. 453–463.

Wideman, R (ed.). 1992. Project and program risk management: a guide to managing project risks and opportunities. Pennsylvania: Project Management Institute. 108 p.

Willem, R. 1988. On knowing design. Design Studies, Vol. 9, pp. 223–228.

Vleck, C. & Stallen, J. 1981. Judging risks and benefits in the small and in the large. Organizational Behaviour and Human Performance, Vol. 28, pp. 235– 271.

Østerås, T. 1998. Design for Reliability, Maintainability and Safety: Procedures and Methods for Conceptual Design. Trondheim: NTNU. 216 p. (NTNU-rapport 1998:23.)

Content of the determination document

Chapter	Examples of things to be documented
Limits of the machine	– Intended use – Possible unexpected functioning – Foreseeable misuse – Etc.
Life cycle of the machine	– Life time – Phases of the life cycle – Etc.
Hazards	– Hazards and ergonomic problems of similar machines (mechanical hazards, noise, vibration, etc.) (see EN 1050 1997)
Environment	– Temperature, pressure, humidity, dirt – Corrosion – Lighting – Radiation – Etc.
Materials	– Process – Cleaning – Lubrication – Exhaust – Structures – Etc.
Lifting and materials handling	– Machine, components, devices – Materials – Personal equipment – Etc.
Working space	– Installation of the machine – Walkways – User position – Etc.
Power transmission	– Gears, axles, couplings, belts, ropes, chains – Pressure lines, electric lines – Springs, pressure accumulators, capacitor – Etc.
Machine actuators	– Cylinders – Motors – Coils – Etc.
Guards and other safety measures	– Guards – Emergency stops – Warnings, markings, instructions – Personal protective equipment – Etc.
Energy	– Mechanical, hydraulic, pneumatic – Electric, chemical – Etc.
Machine functioning	– Functions – Controls – Information – Etc.
Work tasks	– Manufacturing – Transportation – Installation – Use, disturbance control, cleaning – Maintenance – Disposal – Etc.

Risk assessment form

Identification of the hazards, hazardous situations, possible accidents and losses	Risk estimation	Risk evaluation	Is the machine safe?	Further actions
High-pressure water jet, cuts the user's finger or arm during the cleaning of the cutting head.	Sever injury (amputation) Exposure to hazard is low Accident is difficult to avoid due to the difficulty of seeing the water jet	The user may loose his/her finger. The water jet can also cut the whole arm. Therefore additional safety measures are needed	No	Safety design specification
High pressure water jet, cuts the user's finger or arm due to the unexpected startup of the pump unit	" + eye injuries	"	No	Safety design specification
Leakage of high-pressure water hose causes crushes and wounds.	" + eye injuries	"	No	Safety design specification
Fastening of the cutting head fails causing free swing of cutting head and water jet	Severe injury (amputation, severe wounds, eye injury, death) Exposure to hazard is low Accident is difficult to avoid due to the difficulty of seeing the water jet and the fast movements of the free cutting head	"	No	Safety design specification

Safety design specification form

Safety design problem **Legal requirement or standard**	**Safety measure**						
	Hazards elimination	Risk reduction	Safety devices	Warnings	Markings	Instructions	Tests
High-pressure water jet cuts user's finger or arm during the cleaning of the cutting head			The distance between the cutting head and the cutting table is less than 4 mm preventing the user from reaching the water jet	General warning about the water jet		Instructions for maintenance The distance must be less than 4 mm	
High-pressure water jet cuts user's finger or arm due to the unexpected start-up of the pump unit	Common isolation of the electricity of the pump unit and the cutting unit					Instructions for maintenance The main power must be switched off and locked	
Leakage of high-pressure water hose causes crushes and wounds			The control system stops the pump unit in a case of leakage				

Hazards of the proposal for a new draft of the directive on machinery

Part of Annex 1 of the proposal for a new draft of the directive on machinery	Related hazards and hazardous situations
1.2 Principles of safety integration and ergonomics	
1.2.1 Principles of safety integration	– Risks of intended and normal use – Risks of foreseeable abnormal conditions – Risks of use which could reasonably be expected – Risks of accidents throughout the foreseeable lifetime of the machinery including – Assembly – Dismantling – Destruction (withdrawal from service) – scrapping – The constraints to which the operator is subjected when using the personal protective equipment – Risks caused by the lack of special equipment and accessories needed in adjusting, maintenance and use
1.2.2 Machinery ergonomics	
1.2.2.1 General ergonomics	– Discomfort – Fatigue – Psychological stress faced by the operator – The differences in size and strength between man and woman – Dangerous environment
1.2.2.2 Additional requirements for machinery presenting hazards due to mobility	– Hazards related to insufficient visibility, when operating the machinery and its tools in their intended conditions of use – Hazards due to inadequate direct vision – hazards related to inadvertent contact with wheels or tracks – Vibration transmitted to the operator – Rollover of the machine – Hazards related to transportation and working of the operators other than the driver
1.3 Materials	
1.3.1 General requirements	– Hazards caused by – construction materials – used materials – produced materials – Hazardous situations – Filling – Use – Recovery – Draining
1.3.2 Additional requirements for agri-foodstuffs machinery and machinery intended for use in the cosmetics and pharmaceutical industry	– Infection – Sickness – Contagion
1.4 Lighting	
1.4.1 General requirements	– Shadows causing nuisance – Irritating dazzle – Dangerous stroboscopic effects
1.4.2 Additional requirements for machinery presenting hazards due to mobility	
1.4.3 Additional requirements for machinery intended to be used in underground working	

Part of Annex 1 of the proposal for a new draft of the directive on machinery	Related hazards and hazardous situations
1.5 Design of machinery to facilitate its handling	– Hazards related to the handling of machinery or components of machinery – Hazards related to the storing of the machinery or components of machinery (stability etc.) – Sudden movements during transportation – Instability during transportation
2 Controls	
2.1 Control devices	
2.1.1 General requirements	– Hesitation or loss of time and ambiguity in operation – Control devices are located inside hazard zone – Hazards caused by the position of the control devices – Unintentional use of desired, but hazardous, effect – Hazards related to operation of the machine – Starting the machine when persons are in the danger zone
2.1.2 Additional requirements for machinery presenting hazards due to mobility	– Hazards related to the operation of the machine in the driving position – Confusing pedals – Dangerous movements during the operation of pedals
2.1.3 Additional requirements for machinery presenting load-lifting hazards moved by power other than human strength	
2.1.4 Additional requirements for machinery presenting hazards due to the lifting or moving of persons	– Movements of machinery
2.1.5 Additional requirements for construction site hoists	– Excess speeds
2.1.6 Additional requirements for machinery intended to be used in underground working	
2.1.7 Additional requirements for remote-controlled machinery	
2.2 Principle of design of control systems	– Insufficient reliability
2.2.1 Starting of machinery	
2.2.1.1 General requirements	
2.2.1.2 Additional requirements for portable hand-held and/or hand-guided machinery	
2.2.1.3 Additional requirements for certain machinery presenting hazards due to mobility	
2.2.1.3 (a) Self-propelled machinery with a ride-on driver	
2.2.1.3 (b) Movement of pedestrian-controlled machinery	– Inadvertent movements towards the driver – Crushing – Hazards caused by rotating tools
2.2.2 Rules on the stopping of machinery	
2.2.2.1 Normal stopping of machinery	
2.2.2.1 (a) General requirements	
2.2.2.1 (b) Additional requirements for machinery for working with wood, meat and analogous materials	
2.2.2.1 (c) Additional requirements for machinery presenting hazards due to mobility	
2.2.2.1 (d) Additional requirements for machinery intended to be used in underground working	
2.2.2.1 (e) Additional requirements for remote-controlled machinery	
2.2.2.1 (f) Additional requirements for portable hand-held and/or hand guided machinery	
2.2.2.2 Emergency stop	
2.2.3 Mode selection	
2.2.4 Failure of the power supply	
2.2.4.1 General requirements	

Part of Annex 1 of the proposal for a new draft of the directive on machinery	Related hazards and hazardous situations
2.2.4.2 Additional requirements for mobile machinery	
2.2.5 Control circuit failure	
3 Protection against mechanical hazards	
3.1 Stability	
3.1.1 General requirements	– Overturning – Falling – Unexpected movements
3.1.2 Additional requirements for portable and/or hand-guided machinery	
3.1.3 Additional requirements for machinery for working with wood and analogous materials	
3.1.4 Additional requirements for machinery presenting a hazard due to a lifting operation	– Dangerous movements caused by overloading – Exceeded working loads – Exceeded moments caused by the loads – Exceeded overturning moment
3.1.5 Additional requirements for construction site hoists	
3.1.6 Additional requirements for machinery intended to be used in underground working	
3.1.7 Additional requirements for machinery presenting hazards due to mobility	– Rolling over of self-propelled machinery with a ride-on driver
3.2 Risk of break-up during operation	– Flying fragments – Sudden movements – High-pressure jets
3.2.1 General requirements	
3.2.2 Additional requirements for load-lifting machinery	– Failure from fatigue – Failure from wear – Working environment – Corrosion – Abrasion – Impacts – Cold brittleness – Ageing
3.2.3 Additional requirements for lifting and slinging accessories	
3.2.3 (a) Pulleys, drums, chains or ropes	
3.2.3 (b) Slinging accessories	
3.2.4 Additional requirements for construction site hoists	– Falling of the load platform
3.2.5 Additional requirements for cables for use in installations guided by cable	
3.2.6 Additional requirements for machinery intended for lifting or moving persons	
3.3 Risks due to falling or ejected objects	
3.3.1 General rule	– Falling objects – Ejected objects
3.3.2 Additional requirements for machinery for working wood	– Ejection of pieces of wood
3.3.3 Additional requirements for machinery presenting hazards due to mobility	
3.3.4 Additional requirements for construction site hoists	– Falling objects endanger person
3.4 Risks due to surfaces, edges or angles	
3.5 Risk related to combined machinery	
3.6 Risks relating to variations in the rotational speed of tools	
3.7 Risks related to moving parts	
3.7.1 General requirements	– Contacts with hazardous moving parts – Accidental blockage of moving parts
3.7.2 Additional requirements for machinery for working with wood and analogous materials	

Part of Annex 1 of the proposal for a new draft of the directive on machinery	Related hazards and hazardous situations
3.7.3 Additional requirements for machinery presenting hazards due to mobility	
3.7.3 (a) Risks due to towing devices	– Accidental disconnection
3.7.3 (b) Risks due to transmission of power between self-propelled machinery (or tractor) and recipient machinery	
3.7.4 Additional requirements for the engines of machinery presenting hazards due to mobility	
3.7.5 Additional requirements for lifting equipment	
3.7.5 (a) Control of movements	– Amplitude of the movements of components – Collision – Dangerous creep of loads – Free or unexpected fall of loads
3.7.5 (b) Risks due to the movement of loads handled	– Collision with persons – Collision with equipment – Collision with other machinery – Blow from load or counter-weights
3.7.5 (c) Movement of loads handled by machinery powered other than by human strength	
3.7.6 Additional requirements for construction site hoists	– Platform crushes person – Person is trapped by the load platform
3.8 Principles guiding the choice of protection against risks related to moving parts	
3.8.1 Moving transmission parts	
3.8.2 Moving parts directly involved in the process	
4 Required characteristics of guards and protection devices	
4.1 General requirements	
4.2 Additional requirements for guards	
4.2.1 Fixed guards	
4.2.2 Movable guards	
4.2.2 (A) Type A movable guards must…	
4.2.2 (B) Type B movable guards must…	
4.2.3 Adjustable guards restricting access	
4.3 Additional requirements for protection devices	
5 Protection against other hazards	
5.1 Electricity supply	– Electricity
5.2 Electrostatic discharges	– Electrostatic discharges
5.3 Energy supply other than electricity	– Hydraulic – Pneumatic – Thermal – Etc.
5.4 Errors of fitting	– Hazards caused by faulty connection
5.5 Extreme temperatures	– High temperature – Low temperature – Ejection of hot material – Ejection of cold material
5.6 Fire	
5.6.1 General requirements	– Risk of fire posed by – Machinery – Gases – Liquids – Dusts – Vapours – Other substances
5.6.2 Additional requirements for mobile machinery	

Part of Annex 1 of the proposal for a new draft of the directive on machinery	Related hazards and hazardous situations
5.6.3 Additional requirements for machinery intended for use in underground working	– Highly flammable parts – Sparks and fires caused by the braking system
5.7 Explosion	– Explosion posed by – Gases – Liquids – Dusts – Vapours – Other substances
5.8 Noise	– Airborne noise
5.9 Vibration	– Vibration
5.10 Radiation	– Emission of radiation
5.11 External radiation	– External radiation interferes operation of machinery
5.12 Laser equipment	– Laser radiation
5.13 Emissions of dust, gases, vapours, liquids, substances and waste	– Emissions of – Dust – Gases – Vapours – Liquids – Substances – Waste materials
5.13.1 General requirements	
5.13.2 Additional requirements for machinery presenting hazards due to mobility	
5.13.2 (a) Batteries	– Electrolyte being ejected on the operator in the event of rollover – Accumulation of vapours in places occupied by operators
5.13.2 (b) Emissions of dust, gases, etc.	– Exhaust gases – Lack of oxygen – Emission of dust, gases etc.
5.13.3 Additional requirements for machinery intended for use in underground working	
5.14 Risk of being trapped in machinery	– Risk of being trapped in machinery
5.15 Risk of slipping, tripping or falling	– Slipping – Tripping – Falling
5.15.1 General requirements	
5.15.2 Additional requirements for machinery intended for lifting or moving persons	
5.15.2 (a) Risks of persons falling from the carrier	– persons falls from the carrier
5.15.2 (b) Risks of the carrier falling or overturning	– Carrier falls – Carrier overturns
5.15.3 Additional requirements for construction site hoists	– Falling of the loadplatform – Overturn of the loadplatform – Uncontrolled moving upwards of the loadplatform
5.16 Additional requirements for certain machinery	
5.16.1 Agri-foodstuffs machinery and machinery intended for use in the cosmetics and pharmaceuticals industries	– Infection – Sickness – Contagion
5.16.2 Machinery presenting hazards due to mobility	
5.17 Access to workstations	
6 Maintenance	
6.1 Machinery maintenance	– Adjustment, lubrication and maintenance points inside danger zones – Frequent change of components
6.2 Access to servicing points	
6.3 Isolation of energy sources	– Risk of remaining (stored) energy
6.4 Operator intervention	

Part of Annex 1 of the proposal for a new draft of the directive on machinery	Related hazards and hazardous situations
6.5 Cleaning of internal parts	– Dangerous substances
7 Information, warning devices, signals, markings and instructions	– Faults of unsupervised machinery
7.1 Warning devices	
7.1.1 General requirements	
7.1.2 Additional requirements for mobile machinery	– Impacts or crushing caused by remote-controlled machinery – Movements of the machinery – Tools of the machinery
7.2 Warning of residual risks	– Risks that are not evident – Electrical cabinets – Radioactive sources – Bleeding of hydraulic circuits – Hazards in unseen area – Etc.
7.3 Marking, signs, identification	
7.3.1 Marking of products referred to in Article1(1)	
7.3.1.1 General rule	– Risk caused by wrong housing of moving parts
7.3.1.2 Additional requirements for machinery presenting hazards due to mobility	
7.3.1.3 Additional requirements for machinery presenting a hazard due to a lifting operation	– Risk of falling due to unexpected start-up
7.3.1.4 Additional requirements for machinery presenting a hazard due to the lifting or moving of persons	
7.3.2 Additional markings on lifting accessories	
7.4 Instructions	
7.4.1 General	
7.4.1.1 Assembly instructions	– Risk to health and safety of persons
7.4.1.2 General principle for drafting instructions	– Normal use – Uses which can reasonably be expected – Non-professional users
7.4.1.3 Original instructions and translation thereof	
7.4.1.4 Administrative information	
7.4.1.5 Information and warnings concerning product safety	
7.4.1.5 (a) Essential information for operators	– Risks related to opening of blockage
7.4.1.5 (b) Information concerning airborne noise emissions by machinery	
7.4.1.5 (c) Information concerning the risk of lack of stability	– Risk of lack of stability
7.4.1.6 Additional information for certain machinery	
7.4.1.6 (a) Instructions for agri-foodstuffs machinery and machinery intended for use in the cosmetics and pharmaceutical industries	
7.4.1.6 (b) Instructions for mobile machinery presenting hazards due to mobility	
7.4.1.6 (c) Instructions for interchangeable equipment for use with machinery	
7.4.1.6 (d) Instructions for load-lifting machinery	
7.4.1.6 (e) Instructions for machinery presenting hazards due to ionising radiation	
7.4.1.7 Instructions for lifting accessories	
7.4.1.7 (a) General requirements	
7.4.1.7 (b) Additional information for chains and ropes	

Published by

Vuorimiehentie 5, P.O.Box 2000, FIN-02044 VTT, Finland
Phone internat. +358 9 4561
Fax +358 9 456 4374

Series title, number and report code of publication
VTT Publications 411
VTT–PUBS–411

Author(s)
Kivistö-Rahnasto, Jouni

Title

Machine safety design

An approach fulfilling European safety requirements

Abstract

Deficiencies in ergonomics and safety cause negative consequences for companies, national economy and individuals and therefore safer and more healthy products and work environments are required. Improvements in ergonomics and the safety of existing workplaces increase job satisfaction, decrease absenteeism and accidents in companies and may also have positive effects on the quality of the products of companies.

Hazard analysis and risk assessment are widely accepted in product and process design. In the European Union legislators have shifted away from the application of detailed safety requirements towards requirements for application of risk analysis by companies themselves. Manufacturers or their representatives must carry out risk assessment and take results into account in machine design (Directive 98/37/EC). The new regulations are harmonised machine safety requirements within the EU member states and make it possible to market machines throughout the EU.

Today, when the revision of the directive is being considered, it is essential to integrate current safety design procedures into systematic machine design processes in order to ensure both an acceptable level of safety in machines and feasible design efforts. This work was carried out in order to integrate European safety requirements into the systematic machine design process. At the beginning of the work, the theoretical framework was described and the first version of the approach was developed. The preliminary approach was tested and further developed in case studies. The case studies cover the redesign of two existing single machines, the design of a large materials handling system and the safety design of a new single machine.

The main benefit of the approach fulfilling the European safety requirements was the clarification of the safety design requirements and simultaneous safety design together with other design tasks. The results also indicated that the harmonised C-level standards do not necessarily cover all the essential safety problems related to the machine to be designed and therefore risk assessment is recommended even if the C-level standard is available. In addition, the risk estimation according to EN 954-1 (1997) was unreliable. Individual judgements regarding the severity of consequences and the possibility of a user to avoid accident varied drastically. Finally, the machinery safety directive (Directive 98/37/EC) mixes hazards, technical requirements and safety goals in a confusing manner. Therefore, the proposal for a new draft of the directive on machinery (Proposal for... 1998) should be changed in a such way that it clearly separates the hazards, the technical requirements and the safety goals.

Keywords

machine safety, safety design, risk assessment, safety requirements, hazards, risks, machine design

Activity unit

VTT Automation, Risk Management, Tekniikankatu 1, P.O.Box 1306, FIN-33101 TAMPERE, Finland

ISBN			Project number
951–38–5561–9 (soft back ed.) 951–38–5562–7 (URL: http://www.inf.vtt.fi/pdf/)			A9SU00249
Date	Language	Pages	Price
March 2000	English	99 p. + app. 9 p.	C

Name of project	Commissioned by
	Finnish Work Environment Fund, Tampere University of Technology, Technical Research Centre of Finland
Series title and ISSN VTT Publications 1235–0621 (soft back ed.) 1455–0849 (URL: http://www.inf.vtt.fi/pdf/)	Sold by VTT Information Service P.O.Box 2000, FIN–02044 VTT, Finland Phone internat. +358 9 456 4404 Fax +358 9 456 4374